International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.197

(11/2005)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Cable modems

High level requirements for a Digital Rights Management (DRM) bridge from a cable access network to a home network

ITU-T Recommendation J.197

ITU-T

ITU-T Recommendation J.197

High level requirements for a Digital Rights Management (DRM) bridge from a cable access network to a home network

Summary

This Recommendation defines the requirements of a Digital Rights Management bridge from a cable access network to a home network, to which many types of content (e.g., video, audio, etc.) may be transferred by the network operator with assurance that the content is not used in a manner that is a violation of any service agreements or legal requirements.

Source

ITU-T Recommendation J.197 was approved on 29 November 2005 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

ITU-T Recommendation J.197

High level requirements for a Digital Rights Management (DRM) bridge from a cable access network to a home network

1 Scope

This Recommendation defines the requirements of a Digital Rights Management bridge from a cable access network to a home network, to which many types of content (e.g., video, audio, etc.) may be transferred by the network operator with assurance that the content is not used in a manner that is a violation of any service agreements or legal requirements.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– NIST FIPS 140-2 (2002), *Security requirements for cryptographic modules*.

2.2 Informative references

– ITU-T Recommendation J.192 (2005), *A residential gateway to support the delivery of cable data services*.

– DTCP (2005), *Digital transmission content protection specification volume 1 (information version)*.

– Intel (2005), *High-bandwidth digital content protection system, revision 1.1*.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 analogue protection system bits (APS bits): Bits 3 and 2 of the CCI, designating the state of analogue protection for a set top box.

3.2 compliance rules: The rules which apply to set top boxes for the purpose of preventing the unauthorized copying of controlled content.

3.3 consensus watermark: A standard watermark that has been developed for use in DRM.

3.4 constrained image: The visual equivalent of not more than 520 000 pixels per frame (e.g., an image with a resolution of 540 vertical lines by 960 horizontal lines for a 16:9 aspect ratio). A constrained image can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

3.5 constrained image trigger (CIT): The field or bits used to trigger the output of a "constrained image" in the high definition analogue output of set top boxes.

3.6 content protection: The application of technical safeguards that prevent the unauthorized replication and/or redistribution of network delivered content.

3.7 controlled content: Content that has been transmitted from a video service provider's network with the encryption mode indicator (EMI) bits set to a value other than zero, zero (0,0) ("copying not restricted").

3.8 copy control information (CCI): A one-byte field that contains information that set top boxes use to control copying of content. See Annex A for further details.

3.9 digital rights management (DRM): The definition, management, and enforcement of a set of content usage rules. These usage rules will indicate things such as the right to copy, view, or distribute a particular piece of content.

3.10 digital transmission content protection (DTCP): The method of encryption, decryption, key exchange and renewability that is described in the specification entitled "5C digital transmission content protection release 1.0".

3.11 DRM bridge: The distribution and home network infrastructure and technologies put in place to enable content protection and Digital Rights Management for network delivered content being stored and distributed on a home network.

3.12 encryption mode indicator bits (EMI Bits): Two bits, associated with protected content, that specify the copy operations that are permissible for the associated content.

3.13 high definition analogue form or output: A format or output that is not digital, and has a resolution higher than standard definition analogue form or output.

3.14 high-bandwidth digital content protection (HDCP): The method of authentication, encryption, decryption, and renewability that is described in the specification entitled "High-bandwidth digital content protection system, rev. 1.1".

3.15 product: A device and/or technology that receives and possibly distributes content with redistribution control and/or copy control.

3.16 robustness rules: The rules described in clause 6, which apply to set top boxes, and are for the purpose of resisting attempts to modify set top boxes to defeat the functions of the compliance rules.

3.17 service: The video, audio, or data signals, whether in analogue or digital format, transmitted over the video service provider network to (or from) the set top box, for the purposes of effectuating the reception or transmission of information, entertainment, or communications content.

3.18 set top box (STB): Any device that receives content directly from a video service provider, this includes both devices that are separate from the display device, and display devices that have the proper embedded functionality. The STB functions as the service gateway for the home network and includes the conditional access (CA) system and a Digital Rights Management (DRM) system.

3.19 standard definition analogue form or output: A format or output that is not digital (e.g., PAL RF, NTSC RF, Composite, S-Video, YUV, Y, R-Y, B-Y or RGB) and has no more than 483 interlace or progressive active scan lines.

3.20 video content protection system (VCPS): For recording encrypted content on DVD+RW and DVD+R optical digital media protected by VCPS technology.

3.21 video service provider (VSP): A service provider offering a "service" as defined in this Recommendation.

4 Abbreviations, acronyms and conventions

This Recommendation uses the following abbreviations:

AES	Advanced Encryption Standard
APS	Analogue Protection System
CCI	Copy Control Information
CGMS-A	Copy Generation Management System Analogue
CIT	Constrained Image Trigger
DRM	Digital Rights Management
DTCP	Digital Transmission Content Protection
DVD-RW	Digital Versatile Disk – Re-Writable
DVD+R	Digital Versatile Disk + Recordable
DOCSIS	Data Over Cable Service Interface Specification
DVI	Digital Visual Interface
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMI	Encryption Mode Indicator
HDCP	High-Bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
IP	Internet Protocol
LSB	Least Significant Bit
MPEG	Moving Picture Experts Group
NTSC RF	National Television System Committee Radio Frequency
OOB	Out of Band
PAL	Phase Alternate Line
PCI	Peripheral Component Interface
PCMCIA	Personal Computer Memory Card International Association
QoS	Quality of Service
RF	Radio Frequency
RGB	Red, Green, Blue
SRM	System Renewability Message
STB	Set Top Box
S-Video	Super-Video
VCPS	Video Content Protection System
VSP	Video Service Provider
WTSA	World Telecommunication Standardization Assembly

5 Overview

Home networking technology and acceptance has evolved to the point that a home network can serve as a compelling entertainment network, allowing a user to store and distribute content among various home-networked devices. It is in the interest of the industry to leverage this environment in extending entertainment service delivery to the home network. Because cable services often involve high-quality copyrighted content, the need arises to define mechanisms to protect the content and to apply associated usage rules, for a variety of legal and business reasons. This Recommendation establishes the requirements of a Digital Rights Management bridge from a cable access network to a home network, to which content may be transferred by the network operator with assurance that the content is not used in a manner that is a violation of any service agreements or legal requirement.

5.1 Key goals

The goals for the implementation of the DRM bridge include the following:

- Sufficiently robust from the content provider's point of view.
- Non-intrusive from the subscriber's point of view.
- In-tune with the regulatory and legislative environment.

5.2 Key features

Following are the key features for the DRM bridge:

- Authentication of all devices participating in the transmission and/or consumption of video content.
- Extension of a rich set of Digital Rights Management content protection business rules (copy restrictions, number of plays, time-limits, etc.) that have been established as part of the STB.
- Encryption/decryption of video content for transmission/consumption.

5.3 Key technical points

Following are a number of key technical points for the DRM bridge:

- The DRM bridge extends key elements of the DRM to points outside of the STB.
- The DRM bridge supports transmission and storage of both cable-operator delivered content and non-cable-operator delivered content.
- Content with redistribution or copy control may only exit the STB or downstream elements through approved outputs.
- Content without redistribution or copy control may be consumed and stored within the STB or downstream elements.
- Content without redistribution or copy control may freely exit the STB or downstream elements.

5.4 DRM bridge general requirements

G-1	**subscriber-friendly**: DRM bridge shall be transparent to the subscriber, allowing for convenient content consumption, and presenting no barriers to use.
G-2	**simple usage model**: The DRM bridge will employ a simple usage model, allowing purchased network-operator delivered content to be used within the home network in accordance with the rights given to the content.
G-3	**content protection**: The DRM bridge shall prevent unauthorized transmission and copying of protected content outside a home network.
G-4	**block theft-of-service**: The DRM bridge shall prevent theft-of-service and protect the content usage rules (for example, theft-of-content on a wireless network in a multiple dwelling unit).
G-5	**compatible with other DRM technologies**: The DRM bridge shall not preclude the use of other content protection technologies for non-cable operator delivered content.
G-6	**transport agnostic**: The technology used to implement the DRM bridge shall be independent of home networking technologies.
G-7	**backward compatible**: The DRM bridge technology shall not affect existing video-distribution business.
G-8	**distribution agnostic**: The DRM bridge must support various distribution technologies, including MPEG broadcast, IP streaming, and FTP.
G-9	**real time protection**: The technology used to implement DRM bridge shall be applicable to media in real time (for example for broadcast MPEG and IP streaming sources).
G-10	**integrated**: DRM bridge technology and processes should be compatible with other relevant industry initiatives such as DOCSIS (ITU-T Recs J.112/J.122), IPCablecom (ITU-T J.16x and J.17x-series Recommendations) and IPCable2Home (ITU-T J.19x-series Recommendations).
G-11	**open specification**: The specification of DRM bridge shall enable interoperability among equipment from various vendors.
G-12	**economically feasible**: The cost to implement, maintain, validate, and enforce DRM bridge technology and processes should enable feasible business models.
G-13	**dynamically manageable**: Information used to protect content shall be dynamically configurable and manageable.
G-14	**renewability**: DRM bridge security software shall be renewable.
G-15	**functional during outage**: The distribution of controlled and uncontrolled content to the home network shall be supported when access to the conditional access system is impaired.
G-16	**unprotected content**: The DRM bridge should have no impact on the use of unprotected content.
G-17	**extent of content protection**: Content protection shall be available, as established by a DRM rule set, for all video transmissions on the home network.
G-18	**DRM rule set extension**: A rich set of DRM rules (copy, playback, view time, etc.) is provided in the DRM and must be managed by the STB and extended to downstream elements.
G-19	**client authentication**: Authentication shall be supported for all home-networked elements participating in the transmission and/or consumption of video content.
G-20	**encryption**: Content encryption shall be provided for video transmissions within the home network.
G-21	**device revocation**: The ability to deny content accessibility to a particular device shall be provided, even if that device was at one time a valid DRM bridge network element.

5.5 Background

When dealing with the delivery of protected content via a secure distribution network, it is critical that technology is in place to protect the content from unauthorized copying or redistribution. In addition, the device itself must be robust and resistant to security compromise. This Recommendation details content protection technology requirements, and robustness and compliance requirements for devices that handle protected content. These content technology and robustness requirements are written from the perspective of a customer receiving device (i.e., a set top box) that is receiving content from a video service provider as part of a cable distribution network that must protect high-value content. The content is encrypted at the source and is protected throughout the service provider network. The purpose of this Recommendation is to ensure that a comparable level of security is available in home networks. Bridging that content flow into downstream environments in a robust and secure fashion is the focus of this Recommendation.

Content protection and digital output technologies that allow service provider content to exit a set top box must ensure that the service provider still retains control over copying and redistribution of that content, even after the content has exited the set top box to other devices. Devices downstream of the set top box that contain any digital output, DRM, or content protection technology must also comply with the robustness and compliance rules established for the set top box by this Recommendation. The robustness and compliance rules established for the set top box are controlling for the overall downstream ecosystem.

6 Robustness requirements

Devices that receive and possibly distribute protected content must comply with a number of robustness requirements in order to ensure sufficient protection of the content. It is recognized that robustness may vary based on the content available to the device and that the robustness may need to change over time as technology for securing technology, and hacking such technology, changes. This clause outlines a recommended generic set of device robustness requirements.

6.1 Construction

6.1.1 General

Products shall meet the compliance rules and shall be designed and manufactured in a manner to effectively frustrate attempts to modify such Products to defeat the compliance rules.

6.1.2 Defeating functions

Products shall not include:

i) switches, buttons, jumpers, specific traces that can be cut, or software equivalents of any of the foregoing; or

ii) service menus or functions (including remote-control functions),

in each case by which the content protection technologies, analogue protection systems, re-protection, output restrictions, recording limitations, or other mandatory provisions of the compliance rules can be defeated or by which controlled content can be exposed to unauthorized copying. For the purpose of this Recommendation, "re-protection" shall mean the application of an approved, protection technology, when required, to controlled content received from a video distribution network that is to be output from the set top box, and the integrity of the system and methods by which such application is assured.

6.1.3 Keep secrets

In order to frustrate attempts by unauthorized parties to compromise security, products shall be designed and manufactured in a manner to effectively frustrate attempts to discover or reveal:

i) the unique number, of a specified bit length, assigned to each set top box, or the numbers used in the process for encryption or decryption of controlled content (collectively, "Keys"); and

ii) the methods and cryptographic algorithms used to generate such Keys.

6.2 Controlled content paths

Content shall not be available on outputs other than those specified in the compliance rules and, within such product, controlled content shall not be present on any user-accessible buses (as defined below) in non-encrypted, compressed form. Similarly, unencrypted Keys used to support any content encryption and/or decryption in the product's data shall not be present on any user-accessible buses. A "user-accessible bus" means a data bus which is designed for end user upgrades or access such as PCI that has sockets (or is otherwise user-accessible), SmartCard, PCMCIA, or Cardbus.

6.3 Methods of making functions robust

Products shall use at least the following techniques to make robust the functions and protections specified in this Recommendation.

6.3.1 Distributed functions

The portions of the product that perform authentication, and decryption, and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that controlled content in any usable form flowing between these portions of the product shall be secure to the level of protection described in 6.3.5 from being intercepted or copied.

6.3.2 Software

Any portion of the product that implements a part of the content protection technology in software shall include all of the characteristics set forth in 6.1 and 6.2. For the purposes of this Recommendation, "software" shall mean the implementation of the functions against the requirements established by this Recommendation through any computer program code consisting of instructions or data, other than such instructions or data that are included in hardware. Such implementations shall:

a) Comply with 6.1.3 by any reasonable method including but not limited to encryption, execution of a portion of the implementation in ring-zero or supervisor mode, and/or embodiment in a secure physical implementation, and in every case of implementation in software, using effective techniques of obfuscation to disguise and hamper attempts to discover the approaches used.

b) Be designed to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a modification includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to 6.1 and 6.2. This provision requires at a minimum the use of code with a cyclic redundancy check that is further encrypted with a private key or a secure hashing algorithm.

c) Meet the level of protection outlined in 6.3.5.

d) Be designed to provide protection mechanisms from unauthorized software attacks.

6.3.3 Hardware

Any portion of the product that implements the requirements of this Recommendation in hardware shall include all of the characteristics set forth in 6.1 and 6.2. For the purposes of these robustness rules, "Hardware" shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Recommendation requires that a Product be compliant and that:

i) does not include instructions or data other than such instructions or data that are permanently embedded in such a device or component; or

ii) includes instructions or data that are not permanently embedded in such a device or component where such instructions or data have been customized for such product or component and such instructions or data are not accessible to the end user through the product or component.

Such implementations shall:

a) Comply with 6.1.3 by any reasonable method including but not limited to: embedding Keys, Key generation methods and the cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or the techniques described above for software;

b) Be designed such that attempts to reprogram, remove or replace hardware elements in a way that would compromise the security or content protection features of the technology under evaluation or of the set top box, would pose a serious risk of damaging the product so that it would no longer be able to receive, decrypt or decode controlled content (a component which is soldered rather than "socketed");

c) Meet the level of protection outlined in 6.3.5.

6.3.4 Hybrid

The interfaces between hardware and software portions of a product shall be designed so that they provide a similar level of protection to that which would be provided by a purely hardware or purely software implementation as described above.

6.3.5 Level of protection

The core encryption functions (maintaining the confidentiality of Keys, Key generation methods and cryptographic algorithms, conformance to the compliance rules and preventing controlled content that has been unencrypted from copying or unauthorized viewing) shall be implemented in accordance with the "Level 2" requirements of FIPS 140-2 "Security Requirements for Cryptographic Modules" and, at a minimum, in a way that they:

a) Cannot be reasonably foreseen to be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screw drivers, jumpers, clips and soldering irons ("widely available tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or de-compilers or similar software development tools ("specialized tools"), other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required ("circumvention devices"); and

b) Can only with difficulty be defeated or circumvented using professional tools or equipment (excluding circumvention devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement), such as logic analysers, chip disassembly systems, or in-circuit emulators or other tools, equipment, methods or techniques not included in the definition of widely available tools and specialized tools in a above.

7 Compliance rules

7.1 Introduction

In order to be accepted for attachment to the video service provider's network for the reception of protected content, a device must comply with a number of conditions.

7.2 Outputs

7.2.1 General

Product shall not output content, or pass content received through the service to any output, except as permitted in this Recommendation. For purposes of this Recommendation, an output shall be deemed to include, but not be limited to, any transmissions to any internal copying, recording, or storage device, but shall not include internal non-persistent or transitory transmissions that otherwise satisfy these compliance rules and the robustness rules.

7.2.2 Standard definition analogue outputs

Products with any standard definition analogue outputs shall only output content received through the service, or pass content received through the service if the content is properly protected by conformance to appropriate national or regional standards for copy protection of analogue content.

7.2.3 High definition analogue outputs

Products shall be able to constrain, when required by the CIT CCI bit, the resolution of content that is high definition to be output through a connection capable of transmitting content in high definition analogue form, to a constrained image. Products shall include one or more approved digital outputs. All products shall generate and propagate CGMS-A signals for all HD analogue outputs; but shall not be required to respect the CGMS-A trigger unless required by appropriate legislation or regulation.

7.2.4 Digital outputs

Products with any digital outputs shall only output content received through the service, or pass content received through the service as permitted by this Recommendation. A list of technologies that have been tested for conformance to this Recommendation is contained in Appendix I.

7.2.5 Watermark non-interference

Products and components MUST NOT strip, obscure or interfere with the Consensus Watermark in controlled content that has been decrypted.

7.3 Copying, recording, and storage of controlled content

7.3.1 General

Products, including, without limitation, products with inherent or integrated copying, recording or storage capability shall not copy, record, or store controlled content, except as permitted in this clause.

7.3.2 Mere buffer for display

Products may store controlled content temporarily for the sole purpose of enabling the immediate display of controlled content provided that:

a) such storage does not persist after the content has been displayed; and

b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes.

7.3.3 Copy no more

Products shall not copy, record or store controlled content that is designated in the EMI bits as having been copied but not to be copied further ("copy no more"), except as permitted in 7.3.2 or 7.3.5.2.

7.3.4 Copy never

Products, including, without limitation, such a device with integrated recording capability such as a so-called "personal video recorder", shall not copy controlled content that is designated in the EMI bits as never to be copied ("copy never") except as permitted in 7.3.2 or by the following:

Such a device may internally store such content, including for the purpose of pausing the program, if the stored content is securely bound to the product doing the recording so that it is not removable therefrom and is not itself subject to further temporary or other recording within the product before it is rendered unusable; provided the device is made in compliance with specified robustness requirements to avoid circumvention of such restrictions. When internally storing such content, including for the purpose of implementing pause, as allowed in this clause, the content shall be encrypted and stored in a manner that provides no less security than 128-bit Advanced Encryption Standard (AES).

Products shall be designed and manufactured to be able to obliterate the stored content or render unusable the stored content after a stated period of time, on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis.

7.3.5 Copy one generation

7.3.5.1 Copy function

Products may make a copy of controlled content that is designated in the EMI bits as permissible to be copied for one generation ("copy one generation"), as provided in 7.3.2 or 7.3.4 or provided that the copy:

a) is scrambled, encrypted or uniquely bound to that device, in each case using a form of copy protection that is identified by an amendment to 7.3.5, if any; and

b) is remarked as not to be further copied ("copy no more") in a manner that is identified by an amendment to 7.3.5, if any, and will be effective to prevent such further copies being made by devices capable of receiving a transmission of such remarked data through the outputs identified in 7.2.4. In the absence of either such amendment to 7.3.5, no copy of such controlled content other than as permitted in 7.3.2 or 7.3.4 may be made, except as provided in 7.3.5.2.

7.3.5.2 Move function

A product that makes a copy of content marked in the CCI as "copy one generation" in accordance with 7.3.5 may move such content to a single removable recording medium, or to a single external recording device, only when:

a) the external recording device indicates that it is authorized to perform this move function in accordance with the requirements of this clause, and to copy such controlled content in accordance with the requirements of 7.3.5;

b) such controlled content is marked for transmission by the originating Product as "copy one generation";

c) the controlled content is output over a protected output in accordance with 7.2.2, 7.2.3 or 7.2.4;

d) before the move is completed, the originating product recording is rendered non-useable and the moved controlled content is marked "copy no more";

e) the device to which the removable recording medium is moved is unable or rendered unable to output the controlled content except through outputs authorized by these compliance rules; and

f) the copy is stored:

  i) using an encryption protocol approved by amendment to these compliance rules, which uniquely associates such a copy with a single device so that it cannot be played on another device or, if stored to removable media, so that no further usable copies may be made thereof; or

  ii) otherwise using methods referenced in 7.3.5.1.

The current implementation limits the number of moves to a single move. Additional means of controlling content are under study and could be applied when next-generation DRM systems are defined.

8 Change control

Any material or substantial changes to the technology should be re-evaluated using the criteria and process described herein. Material or substantial changes include, but are not limited to:

1) mapping to a new transport or media;

2) changes in the encoding or treatment of content;

3) changes that may have a material and adverse affect on the integrity or security of the technology;

4) changes in the cryptographic method used (except where the algorithm is unchanged and only the Key length is expanded);

5) changes in the scope of redistribution; and

6) any fundamental change in the nature of the technology.

Annex A

Copy control information

Copy control information (CCI) is passed from the video service provider across the data channel to inform the set top box of the level of copy protection required. The CCI is sent in the clear to the set top box, but the integrity of the information is maintained by authenticating the CCI using a simple protocol. This process is replicated for each element downstream from the set top box.

The one-byte CCI field contains information that the set top box and downstream elements use to control copying of content. Two EMI bits control copying on set top box digital outputs, two APS bits control copying on analogue outputs, one bit as a constrained image trigger, and three bits are reserved.

A.1 Channel change

When a channel change occurs, the set top box shall treat all CP-scrambled content as if the EMI is set to "copy never", but shall not apply image constraint until the new CCI message is received. The set top box shall immediately begin using the values of the CCI when it is received from the video service provider. If a new CCI message is not received within 10 seconds, the set top box shall apply image constraint, as if the CIT bit was set to one. Channel change shall not cause a Key refresh to occur.

A.2 CCI Definition

CCI is a single byte, 8-bit, field conveyed from the set top box to the downstream network elements. Five of the eight bits are defined. The remaining three are reserved. The reserved bits shall be set to zero as shown in Table A.1. The downstream element shall use the reserved bit values received from the video set top box only for execution of the authenticated tunnel protocol described below. The set top box shall ignore the reserved bit values thereafter.

Table A.1/J.197 – CCI Bit assignments

CCI bits #	7	6	5	4	3	2	1	0
VSP sets to	0	0	0	CIT	APS1	APS0	EMI1	EMI0
STB interprets as	rsvd	rsvd	rsvd	CIT	APS1	APS0	EMI1	EMI0

A.3 EMI – digital copy control bits

The two LSBs of the CCI byte are the EMI bits. They shall control copy permissions for digital copies. The EMI bits shall be supplied to any set top box digital output ports for control of copies made from those outputs. The EMI bits are defined in Table A.2.

Table A.2/J.197 – EMI values and content

EMI value	Digital copy permission	Content type
00	Copying not restricted	not "high value"
01	No further copying is permitted	high value
10	One generation copy is permitted	high value
11	Copying is prohibited	high value

A.4 APS – analogue protection system

Bits 3 and 2 of CCI as shown in Table A.1 are the APS bits 1 and 0 respectively. The set top box shall use the APS bits to control copy protection encoding of analogue composite outputs as described in Table A.3.

Table A.3/J.197 – APS value definitions

APS	Description
00	Copy protection encoding off
01	AGC process on, split burst off
10	AGC process on, 2 line split burst on
11	AGC process on, 4 line split burst on

A.5 CIT – constrained image trigger

Bit 4 of CCI as shown in Table A.4 is the CIT bit. The set top box shall use the CIT bit to control image constraint of high definition analogue component outputs.

Table A.4/J.197 – CIT values and application

CIT value	Image constraint application
0	No Image constraint asserted
1	Image constraint required

A.6 Authenticated tunnel protocol

The set top box calculates CCI_auth using the received CCI value and compares it with the CCI_auth value received from the video service provider. Failed equivalence generates an error condition and the set top box sets EMI to 11 and applies image constraint as if the value were equal to 1.

Annex B

Robustness checklist

Before releasing any product, the technology implementer must perform tests and analysis to assure the robustness of the implementation. The robustness checklist below may be used for the purpose of assisting the implementer in performing tests covering certain important aspects of robustness. Inasmuch as the robustness checklist does not address all elements required for the manufacture of a compliant product, the implementer is strongly advised to evaluate thoroughly both its testing procedures and the compliance of its Products.

General implementation questions

1) Has the product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analogue protection systems, output restrictions, recording limitations, or other mandatory provisions of the compliance rules can be defeated or by which controlled content can be exposed to unauthorized copying?

2) Has the product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of controlled content or expose it to unauthorized copying?

3) Has the product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analogue protection systems, output restrictions, recording limitations, or other mandatory provisions of the compliance rules?

4) Does the product have service menus, service functions, or service utilities that can alter or expose the flow of controlled content within the device?

   If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect controlled content.

5) Does the product have service menus, service function, or service utilities that can turn off any analogue protection systems, output restrictions, recording limitations, or other provisions of the compliance rules?

   If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the encryption features of the product (including compliance with the compliance rules).

6) Does the product have any user-accessible buses (as defined in 6.2 of the robustness rules)?

   If so, is controlled content carried on this bus?

   If so, then:

   identify and describe the bus, and whether the controlled content is compressed or uncompressed. If such data is compressed, then explain in detail how and by what means the data is being re-encrypted as required by 6.2 of the robustness rules.

7) Explain in detail how the product protects the confidentiality of all Keys.

8) Explain in detail how the product protects the confidentiality of the confidential cryptographic algorithms used in the product.

9) If the product delivers controlled content from one part of the product to another, whether among software modules, integrated circuits, or otherwise, or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other

so that controlled content is secure from interception and copying as required in 6.3.1 of the robustness rules.

10) Are any content protection functions implemented in hardware?

If Yes, complete hardware implementation questions.

11) Are any content protection functions implemented in software?

If Yes, complete software implementation questions.

Software implementation questions

12) In the product, describe the method by which all Keys are stored in a protected manner.

13) Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

14) In the product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys implemented in software.

15) Describe the method in the product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a product) are created and held in a protected manner.

16) Describe the method being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the content protection functions implemented in software.

17) Describe the method by which the product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in 6.3.2b of the robustness rules. Describe what happens when integrity is violated.

18) To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing content protection functions, and describe the method and results of the test.

Hardware implementation questions

19) In the product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.

20) Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

21) In the product, describe how the confidential cryptographic algorithms and Keys used have been implemented in silicon circuitry or firmware so that they cannot be read.

22) Describe the method in the product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a product) are created and held in a protected manner.

23) Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement content protection functions?

24) In the product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of the product (including the compliance rules and the robustness rules) damage the product so as to render the product unable to receive, decrypt, or decode controlled content?

Appendix I

Digital outputs

There will be a need to test digital outputs for conformance to the requirements established in this Recommendation. The following list of digital outputs have been tested for conformance to this Recommendation, and are provided for information. It is expected that additional outputs will conform to the requirements of this Recommendation in the future.

I.1 Cable Television Laboratories has tested the following output and finds it to be in conformance with this Recommendation:

- **1394 with DTCP**: Product may output controlled content, and pass controlled content to an output, in digital form over IEEE 1394 interfaces, where such output is protected by DTCP. Product must support DTCP "full authentication" and may additionally support DTCP "restricted authentication". If required by the applicable licence for DTCP, content that is *not* controlled content shall be output on the IEEE 1394 output without DTCP protection.

I.2 Cable Television Laboratories has tested the following output and finds it to be in conformance with this Recommendation:

- **DVI/HDMI with HDCP**: Product may output content received through the service, and pass content received through the service to an output, in digital form over DVI, including HDMI interfaces, and where the output always has HDCP active and on. Product must pass all lawfully received HDCP SRMs to HDCP function.

Appendix II

Review criteria

Depending on the specific output or technology submitted, criteria for evaluation should include the following:

II.1 Video transport

Are the defined methods used for translating and delivering CCI from the set top box into the proposed device environment or profile?

i) *Compressed digital outputs*

- Is the original digital compression system utilized on the interface, or is the signal recompressed?
- If recompressed, what system, profile, resolution and data-rates are required?
- If the original compression is preserved, is the full transport multiplex sent over the interface, or is the interface limited to single program streams sent after demux?
- If the output carries the full transport stream, how does the system information (e.g., OOB data) get transported?
- What methods are used to ensure uninterrupted flow of programming across this interface, regardless of other traffic that might be present on the interface (QoS)?
- What is the minimum guaranteed data throughput provided on the interface?
- What methods are used to enable delivery, decoding, or display of analogue and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?
- How are analogue programming services preserved seamlessly on this interface?

ii) *Uncompressed digital outputs*

- What is the minimum guaranteed data throughput provided on the interface?
- How are analogue programming services preserved seamlessly on this interface?
- What methods are used to enable delivery, decoding, or display of analogue and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?

II.2 Security interfaces

- How is the security used on the video transport and how is the transport associated with content protection profiles and the methods for authenticating and protecting the content protection profiles?
- What are the key-generation, key-protection and key-exchange methods used?
- Are there obvious areas where content is in the clear?

II.3 Points of attack and system weaknesses

- Can technology be circumvented somewhere?
- Where are the lowest barriers to be attacked?
- Where will the hacker attack and what resources are required?
- What are possible weaknesses/threats and what is the trade-off of security versus the applied costs?

II.4 Effectiveness of proposed technology

- Does the proposed technology adequately protect content passing through the digital output or being securely recorded or stored for later playback?
- What is the scope of content redistribution? Does the digital output or DRM technology effectively protect content from unauthorized redistribution through localization control or other geographic or user restrictions?

II.5 Security processing

- Are the keys and secrets protected from reading and writing during the cryptographic calculations?
- Are CCI, image constraint, and other controls protected throughout the system design?

II.6 Revocation and renewability of keys

- Does the product provide a system key revocation solution?
- Does the product provide a system key renewability solution?
- What criteria and processes are used for revocation and renewability? Who are the participants in the process?
- What is the minimum and maximum size of the system renewability message (SRM), and what format is it delivered in?
- How is the SRM generally delivered? What operational and infrastructure impacts would the revocation/renewability solution have on a video service provider network (including capital equipment or network upgrades that may be required)? What must a video service provider do to adopt the proposed revocation and renewability solutions?

II.7 New algorithms

- What is the relative strength of the algorithm?
- What is the relative strength of authentication with respect to other technologies?

II.8 Preservation of service integrity

- Does the proposed output/technology interfere with a set top box device meeting its other licensing or testing obligations? Is analogue source switching or high definition pass-through required for the proposed digital output?
- Does the output provide a way to preserve the service provider's navigation and service applications?
- Does the proposed output/technology interfere with other commercially available devices and interfaces?
- Does the proposed output/technology raise interoperability issues with other commercially available devices and interfaces?
- Is the proposed interface interoperable with products from other manufacturers, or is it a proprietary or otherwise exclusive solution?
- Is the interoperability defined by industry standards (which ones?) or license, or both?
- Does the technology require conformance or compliance testing in order to assure interoperability?

II.9 Licensing terms

- The licensing terms should conform to ITU practices and national requirements.

II.10 Overall impact on the video distribution network

- What operational and infrastructure impacts would the proposed technology have on a video distribution network (including capital investment or network upgrades that may be required)?
- What must a video service provider do to adopt the proposed technology solution?

Appendix III

Elements of technology review submission

The technologies covered under this recommended evaluation process include protected digital interfaces, secure recording and content storage and playback, and digital rights management. The specific security measures used by these technologies may vary. Additionally, different output technologies may employ transport mechanisms and protocols that require certain limitations or implementation restrictions. This appendix identifies several crucial elements that should be common to all candidate technologies under investigation, but is not an exhaustive list that precludes other types of information that may be necessary for fully evaluating a particular technology. Submissions must not omit or misrepresent material specifications, facts, or other details necessary to conduct a thorough and accurate review of the technology.

Technologies under review may incorporate mixed elements of protected digital interfaces, secure recording and content storage, and digital rights management technologies. The following clauses outline the recommended elements that should be submitted for the thorough review of candidate technologies.

III.1 Licence terms

The licensing terms should conform to ITU practices and national requirements.

Note on Robustness and Compliance Rules – Devices downstream of the set top box that contain any digital output, DRM, or content protection technology must also comply with the robustness and compliance rules established for the set top box by this Recommendation. The robustness and compliance rules established for the set top box are controlling for the overall downstream ecosystem. As a result, the robustness and compliance rules in any manufacturer's technology licence must not be contradictory to robustness and compliance rules detailed in this Recommendation.

III.2 Security overview

The security specification and documentation should include an introduction and security overview that includes the following:

1) An overview of the security architecture, its components (e.g., packaging server, licence server, client, etc.), their functions, and key interfaces; connectivity requirements for output/security.

2) A detailed block diagram of the security architecture identifying the key components and interfaces necessary to implement the solution from end-to-end, including receiver and other media elements (PCs, storage, display, etc.).

3) This overview should also clearly identify video transport options where there are alternatives in implementation. For example, video transport cipher algorithms (AES, 3-DES, etc.), and key exchange algorithms (Diffie-Hellman, RSA, etc.).

4) A detailed description of the mapping of the set top box content protection rules or licences to the proposed content protection technology to be embedded in "downstream" devices, specifically addressing the issue of maintaining overall security and content protection throughout the distribution ecosystem.

III.3 Video transport

The security specification should include details regarding the video transport method and the specifics of how the copy control information (CCI) presented by the set top box is translated into the proposed environment/profile. The specification should also detail how the video transport is associated with any content protection profiles and the methods for authenticating and protecting the content protection profiles.

In addition, specifications or other technical descriptions must be provided to fully explain how the proposed digital output supports one or more video transport protocols capable of delivering all defined[1] audio-video services associated with a set top box without disrupting, impeding or impairing the delivery of such services to the final display device. Such services also include, but are not limited to delivery, decoding, or display of analogue and digital closed-caption data, content advisory ratings, and emergency alert system messages.

The technology review should be conducted for each transport mechanism and protocol encompassed by the content protection technology. Such reviews should be made on a transport-by-transport, or media-by-media basis. If a particular technology successfully meets the criteria herein, that technology should not be considered as having a "blanket approval" for any transport or protocol.

III.4 Content protection profiles

The security specification should include details regarding the format and use of any digitally signed content protection profiles used in the system. The security specification should also define the structure and options that are employed in this system and all messaging and signalling needed for implementation.

III.5 Key exchange algorithms

The security specification should include details regarding the authentication of receiving devices, storage devices, and any devices connected thereto. The security specification should also include authentication methods of the Licence server, packaging server and the client. All of the session keys exchanged and the cryptographic protocols used should be well defined for a complete review. Non-encryption alternatives may also be employed, but should be explained thoroughly.

III.6 Security interfaces

The specification should include details that completely define the security interfaces of the overall system and the creation and protection of symmetric and asymmetric keys. Detailed definitions of the security components implemented in hardware and software need to be defined so that these security interfaces can be reviewed.

III.7 Security processing

The specification should include details that demonstrate how the keys and secrets are protected from reading and writing during the cryptographic calculations, and how the CCI, image constraint and other parameters are protected throughout the system.

III.8 Certificate management

The specification should include details that completely define the certificate usage, methods for protecting private keys, revocation methods and how certificates relate to content and the packaging/licence servers. Details on installation, signing, chaining to the root, as well as the overall structure, validation of security, and protection against cloning of certificates should be included.

[1] See for example, ANSI/SCTE40-2004; Section 8.1.

III.9 Revocation/renewability of key

The specification should include details on how system key revocation is accomplished, and how key renewability is accomplished.

III.10 Points of attack/potential weaknesses

The specification should include reviews or threat analyses that may be available to review the possible weaknesses/threats and the trade-off versus the applied costs. Independent security reviews should also be provided. As appropriate, non-disclosure restrictions can be put in place to cover the review.

III.11 Commercial use

The submission should include any known commercial use of the proposed output or technology, as well as any known affects on performance of devices, and interoperability issues. The submitter should provide a list of adopters (implementers) and supporters (owners, content developers, etc.), and identify any commercial relationships between the technology submitter and any content owners.

III.12 Contact information

The submission should include the names and contact information for the security specialist and other individuals who may be contacted with questions concerning the submission.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006