

BRAZILIAN
STANDARD

ABNT NBR
15605-1

First edition
2008.10.03

Valid from
2008.11.03

Corrected version
2009.07.16

Digital terrestrial television — Security issues
Part 1: Copy control

Descriptors: Digital terrestrial television. Copyright. Digital rights. Interface protection. HDCP. DTCP.

ICS 33.160.01

ISBN 978-85-07-01042-5



Reference number
ABNT NBR 15605-1:2008
18 pages

© ABNT 2008

ABNT office

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ABNT.

ABNT office

Av. Treze de Maio, 13 - 28º andar

20031-901 - Rio de Janeiro - RJ

Tel.: + 55 21 3974-2300

Fax: + 55 21 2220-1762

abnt@abnt.org.br

www.abnt.org.br

Published in Brazil

Contents

Pages

Foreword.....	v
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviations	3
5 General copy control rules	3
6 Service types.....	4
7 Digital copies	5
7.1 Digital copy control descriptor and content availability descriptor.....	5
7.2 Copy control information priorities	5
7.3 Standard digital copy control information.....	5
8 Content copy control.....	6
8.1 Descriptors.....	6
8.2 Copy control on a digital television service	6
8.3 Copy control for data services.....	6
8.4 Description of the copy options.....	8
8.4.1 Category 1: “copy free”	8
8.4.2 Category 2: “copy free in SD format”	8
8.4.3 Category 3: “copy free in SD format and copy once in original resolution”	8
9 Content recording information.....	9
9.1 Maximum bit rate information	9
9.1.1 Definition for the maximum bit rate value.....	9
9.1.2 Values of the maximum bit rate when the maximum bit rate is not described	9
9.1.3 Specification for maximum bit rate on a television with multi-camera.....	10
9.2 Change of copy control information.....	10
9.3 Copy control restrictions	10
9.3.1 Standard copy control restrictions.....	10
9.3.2 Encryption plus non-assertion bit (encryption_mode).....	10
9.4 Retention of contents.....	11
10 Rules for full-seg receivers	11
10.1 General rules.....	11
10.2 Output control rules	11
10.2.1 Requirements of the output function	11
10.2.2 Output control rules	12
10.2.3 Output control rules with the non-assertion bit encryption.....	12
10.3 Internet transmission rules	13
10.4 Bound recording.....	13
10.4.1 Bound recording limited	13
10.4.2 No more copies.....	13
10.4.3 Retention	13
10.4.4 Move function	14
10.5 Digital recording with the removable recordable media	14
10.6 Analog recording with the removable recordable media	15
11 Robustness rules for the receiver units.....	15
11.1 Basic requirements of robustness rules.....	15
11.2 Implementation methods of robustness	15

ABNT NBR 15605-1:2008

11.2.1	General aspects	15
11.2.2	Content output	15
11.2.3	Storing contents	16
11.3	User accessible bus	16
11.4	Prohibition re-using of copies.....	17
11.5	Actions that shall be prohibited regarding information control.....	17
11.6	Digital recording of contents to the removable recording media	17
12	Output interface	17
12.1	Analog video output interface.....	17
12.2	Digital video output interface	17
12.3	Analog audio output interface.....	17
12.4	Digital audio output interface.....	17
12.5	Other digital output interfaces	17
	Bibliography.....	18

Foreword

The ABNT – Associação Brasileira de Normas Técnicas (Brazilian Association of Technical Standards) – is the Brazilian Standardization Forum. Brazilian Standards, whose content is the responsibility of the Brazilian Committees (Comitês Brasileiros – ABNT/CB), Sectorial Standardization Bodies (Organismos de Normalização Setorial – ABNT/ONS), and Special Studies Committees (Comissões de Estudo Especiais – ABNT/CEE), are drafted by Study Committees (Comissões de Estudo – CE). Such CE committees are made up of representatives from the sectors involved and include producers, consumers, and neutral entities (universities, laboratories, and others).

Technical ABNT Documents are drafted in accordance with the rules given in the ABNT Directives (Diretivas), Part 2.

Attention is drawn to the possibility that some of the elements in this document may be the subject of patent rights. ABNT shall not be held responsible for identifying any patent rights.

ABNT NBR 15605-1 was prepared within the purview of the Special Studies Committee for Digital Television (ABNT/CEE-00:001.85). The Draft Standard was circulated for National Consultation in accordance with ABNT Notice (Edital) nº 07, from July 10, 2008 to August 08, 2008, with Draft number 00:001.85-005/1.

Should any doubts arise regarding the interpretation of the English version, the provisions in the original text in Portuguese shall prevail at all times.

This Standard is based on work carried out by the Brazilian Digital Television Forum as established by Presidential Decree number 5.820 of June 29 2006.

ABNT NBR 15605 under the general title “Digital terrestrial television — Security issues” has the provisions to contain the following parts:

- Parte 1: Copy control;
- Parte 2: Security mechanisms for applications, and
- Parte 3: Extensions.

This English version is equivalent to the corrected version of ABNT NBR 15605-1:2008, from 2009.07.16.

This corrected version of ABNT NBR 15605-1:2008 includes the Technical Corrigendum 1 from 2009.07.16.

Introduction

This part of ABNT NBR 15605 specifies the signaling of the content copy control and its interpretation by the receiver platform in order to reflect them in the output interfaces. International copy control tools are used in order to achieve better interoperability and cost reductions due to large-scale economies.

The scope of this document is the specification of mechanisms that help in the fight against counterfeiting high definition contents and assumes that the use of this signaling on the broadcasting signal complies with the legislation in force and with the Copyright Law.

Changes to the copy control signaling, after the recording in the removable media, is out of the scope of this part of ABNT NBR 15605.

Digital terrestrial television — Security issues

Part 1: Copy control

1 Scope

This part of ABNT NBR 15605 establishes the mechanisms and rules for the copy control using international protection tools applied to the video, audio and data output of the digital terrestrial television system receivers (SBTVD).

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only the editions mentioned apply. For undated references, the latest editions of the referenced document (including any amendments) apply.

ABNT NBR 15603-1:2007, *Digital terrestrial television – Multiplexing and service information (SI) – Part 1: SI for digital broadcasting systems*

ABNT NBR 15603-2:2007, *Digital terrestrial television – Multiplexing and service information (SI) – Part 2: Data structure and definitions of basic SI information*

IEC 60958:2003, *Digital audio interface*

ARIB TR-B14:2006, *Operational guidelines for digital terrestrial television broadcasting. Version 2.8*

HDCP, *High-bandwidth digital content protection system. Revision 1.3.*

DTCP, *Digital transmission content protection specification*

3 Terms and definitions

For the purposes of this part of ABNT NBR 15605, the following terms and definitions apply.

3.1

high definition

definitions above 350000 pixels or 480 progressive lines

3.2

standard definition

definitions up to 350000 pixels or 480 progressive lines

3.3

DTCP

content protection system for content transmission on digital interfaces

3.4

EIT

table that describes program related information such as titles, program duration and synopsis

3.5

limited recording

type of recording that allows content reproduction only on the equipment that recorded the content

3.6

HDCP

content protection system for transmission of digital audio and video signals

3.7

PID

set of 13 that compose the packet identification information of a stream

3.8

PMT

table that indicates the PID program component

3.9

full-seg receiver

devices capable of decoding audio, video, data, etc., carried by the transport stream layer of the thirteen segments designed for fixed (indoor) and mobile service

NOTE The full-seg classification is applied to the digital converter, also called by set-top box, as well as to the 13-segment receiver integrated with the display, but not exclusive to these. This kind of receiver is capable of decoding the signal from the terrestrial digital television in high definition and, according to the manufacturer's criteria, also to decode information carried on layer "A" of the transport stream, applied to services directed to portable receivers, defined here as one-seg.

3.10

one-seg receiver

device capable of decoding audio, video, data, etc information transported on layer "A" that is located at central segment of the 13 segments

NOTE The one-seg classification is designed for portable receiver, also known as handheld, specially recommended for small displays, normally up to 7 inches. Among the products classified as one-seg there is, but not limited to these, a receiver integrated with a cell phone, PDA, dongle and portable TV sets. This kind of receiver is able to receive and decode signals from terrestrial digital television transported on layer "A" and consequently only baseline profile signals designed for portable devices.

3.11

retention

temporary content storage for later visualization (time-shift)

3.12

high-speed digital interface

high-speed data output such as USB, Firewire and Ethernet

3.13

service description table

SDT

table that lists the service information related to the broadcast channel such as the broadcaster and service names

3.14

service

series of programs that can be broadcasted as part of the programming, which is organized per broadcaster

4 Abbreviations

For the purpose of this part of ABNT NBR 15605, following abbreviations apply.

DTCP	Digital Transmission Content Protection
EIT	Event Information Table
EPN	Encryption Plus Non-Assertion
HDCP	High-bandwidth Digital Content Protection
HDMI	High-definition Multimedia Interface
IP	Internet Protocol
MPEG	Motion Picture Experts Group
MPEG_TS	MPEG Transport Stream
PID	Packet Identifier
PMT	Program Map Table
SD	Standard Definition
TS	Transport Stream
USB	Universal Serial Bus

5 General copy control rules

The protection of digital broadcast content is based on the application of rules by the receivers, particularly in the output interfaces. In order to assure the content protection during the signal transmission process, the general rules for copy protection shall be followed in transport stream coding and shall be reflected in the output interfaces of the receivers and in the recorded signals of the different media.

The one-seg receivers are not required to implement copy control signaling interpretation. The corresponding transport stream shall be signaled as “copy free”.

The full-seg services shall implement interpreters to the digital copy control descriptors, which allow restrict copies of high definition content. In the absence of copy control signaling the receiver shall interpret it as “copy free”.

The analog outputs in standard definition of full-seg receivers do not require any protection. In this format, the copy of the signals is always free.

Full-seg receivers that have high definition analog video outputs, called component videos, shall protect the exported content when copy control signaling is different to “copy free”. The interface protection mechanism shall be the reduction of image resolution, constraining it to standard definition.

Full-seg receivers that have digital video outputs shall seek authentication from the device connected to this interface for signal output. If authentication is unsuccessful or if the authentication mechanism is not implemented, the image resolution shall be restricted to standard definition. If the authentication is successful, the content shall be exported and encrypted according with the interface protocol.

The full-seg receivers that have high speed digital outputs shall seek authentication from the device connected to this interface for signal output. If authentication is unsuccessful or if the authentication mechanism is not implemented, the output shall be blocked. If the authentication is successful, the content shall be encrypted and exported.

6 Service types

The transport stream shall contain an identifier for each type of service. The complete list of services used on digital terrestrial broadcasting is shown in ABNT NBR 15603-2:2007, Table 36.

The content protection rules vary depending on the type of service. In this context, the relevant types of services are the following (signaled according to Table 1):

- digital television service: service which contains at least one video stream, and always enables stable reception of programs, even on receivers not equipped with the function to receive the data service;
- data service: service primarily designed for real-time transmission of data contents which contains at least one data carousel;
- special service: service that was prepared for broadcasting at irregular times on different channels to those of regular service channels. This service includes the special video and data services and is not used during regular operation, and where no prior notification is given to viewers regarding this service;
- engineering service: maintenance service for receiver units. This service includes fixing bugs, solving transmission related problems, correcting problems arising from the difference of interpretation in the operation among receiver units, improving the display, accelerating response and improving operability. The service also includes updating logo data of broadcasting companies, the program genre code table, the table of program code characteristics and reservation term commonly applied to all receiver units;
- bookmark of data service list: service that displays the bookmark information recorded in the NVRAM of the receiver units.

Table 1 — Service type information

Service-type	Description
0x01	Digital television service
0xA1	Special video service
0xA3	Special data service
0xA4	Engineering service
0xA8	Data service for anticipated storage
0xA9	Exclusive data service for storage
0xAA	Bookmark of data service list

7 Digital copies

7.1 Digital copy control descriptor and content availability descriptor

The structure of the digital copy control descriptor shall comply with ABNT NBR 15603-1:2007, Figure 42 and its syntax shall be according to ABNT NBR 15603-2:2007, sub-clause 8.3.23. The structure of the content availability descriptor shall comply with ABNT NBR 15603-1:2007, Figure 69 and its syntax shall be according to ABNT NBR 15603-2:2007, sub-clause 8.3.45.

The digital copy control descriptor specifies the rules for content copy and the maximum bitrates used to verify availability and recording mode. Furthermore, the content availability descriptor specifies the current cryptography status of the output signals.

7.2 Copy control information priorities

The digital copy control descriptor and the content availability descriptor shall be present in the first loop of the PMT, in the SDT or in the EIT. The SDT description shall be used when there is no descriptor in the EIT. When the digital copy control descriptor is present in two or three tables, the priority order is PMT > EIT > SDT (PMT has more priority).

In order to specify the copy control information regarding a service, the copy control descriptor shall be present in the SDT. To specify the copy control information regarding each event, the copy control descriptor shall be present in the EIT. When the digital copy control descriptors are present in both the SDT and EIT, the EIT description shall have priority.

7.3 Standard digital copy control information

When a digital copy control descriptor is not present in the PMT, SDT or EIT, the receiver shall interpret this absence as “copy free”, i.e. the receiver shall apply the default value according to the service, as follows:

- for a digital television service and special video service, copy_control_type = ‘01’, digital_recording_control_data = ‘00’, APS_control_data = ‘00’;;
- for data service, special data service copy_control_type, data service of indicators list = ‘01’, digital_recording_control_data = ‘00’, APS_control_data = ‘00’.

In the absence of a content availability descriptor in the PMT, SDT or EIT, when the digital copy control descriptor is sent, the encryption_mode is taken as defined in ‘1’, corresponding to content output encryption.

In the absence of a content availability, or control descriptor in the PMT, SDT or EIT, the encryption_mode is taken as defined in ‘0’, corresponding to non-encryption of the content output from the high-speed digital interface.

In the case of one-seg receivers, regardless of the digital copy information, the interpretation shall be “copy free”.

The resolution bit limitation (image_constraint_token) of the content availability descriptor shall always be defined as ‘1’, with no resolution limitation. In this Standard, the resolution limitation is based on other content availability descriptors and digital copy control fields.

In the absence of the content availability descriptor in the PMT, SDT or EIT, when the digital copies control descriptor is sent, the *retention_mode* is presumed in ‘0’ while the *retention_state* is presumed as defined in “111”, corresponding to the permitted content time accumulation, with no maximum time limit.

In the absence of both the content availability descriptor and the digital copies control descriptor in the PMT, SDT or EIT, the *retention_mode* and the *retention_state* do not apply, as the digital copy control is considered to be “free to copy”, therefore there is no limitation on time accumulation.

8 Content copy control

8.1 Descriptors

The content copy control shall be based on information from the digital copy control descriptor and the content availability descriptor in association with the mechanisms of protection and authentication of the output interfaces of the receiver. These descriptors contain information regarding the conditions of the permission for digital recording.

NOTE The mechanisms for the content protection of the digital video and analog outputs and the high-speed interfaces are defined in this part of ABNT NBR 15605.

When the `copy_control_type` of the digital copy control descriptor is '11' the output in MPEG-TS format is forbidden for any output interface.

When performing the output of audio signals compatible with IEC 60958, no encryption shall be applied.

When the content copy control information is updated, the receiver shall exhibit the content in the original resolution, and shall execute a new authentication with the external device.

8.2 Copy control on a digital television service

Table 2 informs which types of copies are applicable to the context of free-of-charge open digital television. The copy types are defined on `digital_recording_control_data` of the digital copy control descriptor.

Table 2— Operation rules for content protection

Services	Digital copy control information "digital_recording_control_data"			Non-assertion bit encryption_mode
	"Copy free" '00'	"Copy free in SD format" '11'	"Copy free in SD format and copy once on the original resolution" '01'	
Free programs without protected content	Applicable	Applicable	Applicable	Applicable only when "copy free"

The encryption plus non-assertion bit (`encryption_mode`) of the content availability shall be used to protect the "copy free" content from high-speed digital interface output.

8.3 Copy control for data services

The value of the identifiers of these descriptors for the data services shall be according to Table 3 for digital television services, special video services, data, special data service and bookmark of data service list. Combinations not defined in Table 3 are forbidden.

Table 3 — Descriptor values for data service

Categories for copy control	Information of digital copy control for the digital interface	Information of copy control for the analog interface	Digital copy control descriptor			Content availability descriptor	
			copy_control_type	digital_recording_control_data	APS_control_data	encryption_mode	image_constrain_token
"Copy free"	Copy free in standard definition, copy free in high resolution and external MPEG_TS output interface, enabled and not encrypted	Copy free	01	00	00	0	1
	Copy free in standard definition, copy free in high definition and external MPEG_TS output interface, enabled and encrypted					1	1
	Copy free in standard definition, copy free in high definition and external MPEG_TS output interface disabled					1	1
"Copy free in SD format"	Copy free in standard definition, copy free in high resolution and external MPEG_TS output interface enabled ^a	Copy free in standard definition	01	11	Different from 00	1	1
	Copy free in standard definition and external MPEG_TS output interface disabled		11			Different from 00	1
"Copy free in SD format and copy once in original resolution"	Copy free in standard definition, copy one generation in original resolution and external MPEG_TS output interface enabled	Copy free in standard definition	01	10	Different from 00	1	1
	Copy free in standard definition, copy one generation in original resolution and external MPEG_TS output interface disabled		11			Different from 00	1

^a Does not apply to digital television services.

8.4 Description of the copy options

8.4.1 Category 1: “copy free”

Even if “copy free” is defined, the encryption shall be executed in high speed digital output interfaces, according to the DTCP specifications when the encryption_mode value is ‘1’. Encryption is not required on the high speed serial interface when the encryption_mode is ‘0’.

For the remaining output interfaces, analog video and digital video, the content can be exported without any kind of protection.

8.4.2 Category 2: “copy free in SD format”

For the digital television services, special video services, data service, special data service and bookmark of data service list, the DTCP protection shall be applied according to Table 6.

For the DVI and HDMI digital video outputs, when the digital copy control information of category 2 is received, the result of the HDCP protocol authentication shall be verified. If the authentication is successful, then the HDCP encryption with the corresponding signaling shall be applied to the content exported through the digital video interface. However, if the HDCP authentication is unsuccessful or the HDCP protocol is not implemented, the content resolution shall be reduced to standard definition. The digital copy control information of the HDCP protocol for the standard definition content shall become “copy free”.

Whenever the copy control information of category 2 is received, the content resolution exported through the analog interface shall be equivalent to standard definition.

8.4.3 Category 3: “copy free in SD format and copy once in original resolution”

For the digital television services, special video services, data service, special data service and bookmark of data service list, the DTCP protection shall be applied according to Table 6.

For the DVI and HDMI digital video outputs, when the digital copy control information of category 3 is received, the result of the HDCP protocol authentication shall be verified. If the authentication is successful, then the content shall be encrypted and the “copy one generation” signaling shall be applied to the content exported through the digital video interface. However, if the HDCP authentication is unsuccessful or the HDCP protocol is not implemented, the content resolution shall be reduced to standard definition. The digital copy control information of the HDCP protocol for the standard definition content become “copy free”.

If the content of category 3 is stored, then the device shall change the copy control information of the recorded file to “prevent additional copies in high resolution”. This signaling shall be applied from this moment on in all actions related to this content.

Whenever the copy control information of category 3 is received, the content resolution exported through the analog interface shall be equivalent to the standard definition.

9 Content recording information

9.1 Maximum bit rate information

9.1.1 Definition for the maximum bit rate value

The maximum_bit_rate field in the digital copy control descriptor represents 0.25 of the bit rate value in mega bits per second.

EXAMPLE If the value is "0x24", that means, 36 in decimals, the value of the maximum bit rate is 9 Mbps. For a variable bit rate, the value of the maximum rate is described. The value of the maximum bit rate is also described in the PMT and the value does not change in real time when the current bit rate changes.

When the value of the maximum bit rate of a transmitted service exceeds, or is remarkably below, a value shown in Tables 4 and 5, or is not listed in any of these tables, the broadcaster shall define a digital copy control descriptor and describe the value in the field maximum_bit_rate.

9.1.2 Values of the maximum bit rate when the maximum bit rate is not described

The values of maximum bit rates of the transport stream when the maximum bit rate is not described shall comply with Tables 4 and 5. Table 4 indicates the maximum rate for each component of the transport stream and Table 5, the maximum rate for each type of service.

Table 4 —Maximum bit rates values for each component

Component type	Component description	Bit rate
Video	1080i	8 Mbps to 20 Mbps
	720p	8 Mbps to 20 Mbps
	480p	4 Mbps to 12 Mbps
	480i	1.5 Mbps to 8 Mbps
Audio	Standard stereo	330 kbps
	High quality stereo	330 kbps
	5.1 Multichannel	458 kbps
Additional data	----	4 Mbps
Caption, closed caption and superimpose	----	256 kbps

Table 5 — Maximum bit rate values for each type of service

Type of media	Service detail	Bit rate Mbps
Digital television service	1080i	21
	720p	21
	480p	12
	480i	11
	Multi-camera	21
Data service	----	2.2

In the case of a one-seg service, the recording may be performed at the rate used for the transmission of the service, whatever it may be.

9.1.3 Specification for maximum bit rate on a television with multi-camera

The maximum bit rate shall be specified for each event or component by using the digital copy control descriptor, but the maximum bit rate on a multi-camera television service shall be specified with the component group descriptor. So, in an event where a component group descriptor is present, when the `component_group_type` is set to '000' while the `total_bit_rate` value is specified for each group of components, the total bit rate in the group of component descriptors shall be given priority.

9.2 Change of copy control information

Once the copy control information of an event is set, broadcasters shall avoid changing this information.

Specially when the rights management information is changed from “copy free” or “copy free in SD format and copy once in original resolution” to “copy free in SD format”, even a receiver for which the copy was allowed without restrictions when the recording was scheduled, at the time of the recording this shall be done in standard definition (in standard-resolution for “copy free in SD” signaling, or in original resolution with the configuration set from “stop copies in high resolution” to signaling “copy free in SD and once in original resolution”).

If an event has the possibility of changing to “copy free in SD format”, the digital copy control descriptor shall be transmitted in EIT signaling “copy free in SD format”. When it is decided that the program may be copied in high definition, the EIT table shall be updated and the new copy information transmitted.

For the same reason, the content of the copy control information, described in the SDT, shall not be changed carelessly. This is because, when a digital copy control descriptor is not present in the EIT, the information described in the SDT is used, and the recording schedule is made based on that information. To change the copy control information described in the SDT, up to N days before the recording date (when the information for N days is transmitted in SI), the digital copy control descriptors shall be present in the EIT. The EIT tables shall be regularly transmitted to all the programs, so that there are no programs scheduled for recording using the copy and control information in the SDT. Only after this cycle, the copy control information in the SDT may be changed.

9.3 Copy control restrictions

9.3.1 Standard copy control restrictions

The content availability descriptor shall be used in combination with the copy control information in a digital copy control descriptor. When a digital copy control descriptor is not present, the content availability descriptor is not valid. In these conditions, the receiver shall discard the information on the content availability descriptor and consider the content as “copy free”.

9.3.2 Encryption plus non-assertion bit (`encryption_mode`)

The `encryption_mode` is valid for the output of a transport stream on a high-speed digital interface, when the `copy_control_type` is set to '01' and `digital_recording_control_data` is set to '00' (“copy free”). Otherwise the `encryption_mode` is held at '1'. For details of the *encryption_mode* operation, see the DTCP specifications.

9.4 Retention of contents

The concept of retention only has meaning when the copy control information is “copy free in SD format”. Even when the copy control information is “copy free in SD format”, the content can be temporarily stored up to the maximum time allowed for temporary retention.

The retention information is a combination of *retention_mode* and the *retention_state* according to ABNT NBR 15603-2:2007, subsection 8.4.45.

10 Rules for full-seg receivers

10.1 General rules

Full-seg receivers shall implement output functions as defined in 10.2.

If the bound recording is implemented in *full-seg* receivers, the function shall be implemented according to the rules defined in 10.4.

If the removable media recording is implemented, the function shall be implemented according to the rules defined in 10.5 and 10.6.

10.2 Output control rules

10.2.1 Requirements of the output function

The copy control specified in Section 8 shall be applied to the analog and digital video outputs and to the stream output. The audio output on all interfaces has no protection, except the HDMI that shall apply the HDCP when the content is protected.

The DTCP shall be applied to the output of the high-speed digital interface for the exportation of the digital television service, the special video service, the data service, special data service and the bookmark of data service list, when the content indicates that it is different from “copy free”.

The IP interface output shall be according to the DTCP. The IP protocol shall only be unicast. The number of streams output at a time shall be limited to eight, or less, for each reception part. This does not apply to the playback output of bound recorded contents. Contents may be transmitted to the IP interface only when the destined IP address of the transmitted pack is in the same subnet as the IP address of the receiver unit.

Contents may be exported to the analog video output interface according to the specifications of Section 8. In content transmission with an indication different to “copy free”, the video resolution shall be limited to a standard definition.

The “copy free” content may be output through the digital video output or digital video/audio output. For content protected by the digital copy control descriptor and content availability descriptor, the appropriate protection shall be applied to digital video output or digital video/audio output, according to the HDCP specifications.

When the HDCP authentication result indicates the blocking of content, the full-seg receiver shall reduce the video resolution to standard definition. After the resolution is reduced, the content shall be considered as “copy free” until the update of the copy control information, which may occur when the descriptors are updated or in the change of event.

10.2.2 Output control rules

The rules for signal output control, applicable to full-seg receivers shall be according to the `copy_control_type` and `digital_recording_control_data` of the digital copy control descriptor and the `encryption_mode` of the content availability descriptor shall be as indicated in Table 6.

When the DTCP is used in data service, special data service, or bookmark of data service list, the “DTCP descriptor” shall be inserted according to the DTCP specification.

Table 6 — Control rules for the high speed digital interface for digital television services, special video services, data services, special data services or bookmark of data service list

Digital copy control descriptor		Content availability descriptor	High-speed digital interface	
			Serial interface	IP interface
Copy_control_Type	digital_recording_control_Data	encryption_Mode	<i>MPEG_TS</i>	<i>MPEG_TS</i>
01	00	1	No encryption	No encryption
		0	Mode B	Mode D0
	Does not matter	10	Mode B	Mode B0
		01	Mode C	Mode B0
		11	Mode A	Mode A0
11	00	Does not matter	No encryption	No encryption
	10		No output	No output
	01			
	11			
10	Does not matter	Does not matter	No output	No output
00				
No descriptor			No encryption	No encryption

Details of the high-speed digital interface output mode (mode A, B, C, A0, B0 and D0) shall be according to the DTCP specification, considering the differences between the serial and IP interfaces.

10.2.3 Output control rules with the non-assertion bit encryption

When the digital copy control descriptor and content availability descriptor are transmitted, the high-speed digital interface output shall be controlled according to Table 6 with the non-assertion bit encryption of the content availability descriptor and the information of the digital copy control descriptor.

When `copy_control_type` and `digital_recording_control_data` of the digital copy control descriptor are set to ‘01’ and ‘00’ respectively, the non-assertion bit encryption shall be enabled. In this case, the high-speed digital interface output shall be encrypted according to Table 6.

To transmit a partial transport stream to the high-speed digital interface when the content availability descriptor is transmitted and `copy_control_type` of the digital copy control descriptor is set to ‘01’, the EPN bit of the DTCP_descriptor shall also be set according to the information of the non-assertion bit encryption.

10.3 Internet transmission rules

The receiver units shall not be allowed to enable the outputs for retransmission through the Internet. The outputs specified in Section 12 are allowed.

In order to restrict the transmission via the Internet, the user-accessed I/O bus and recordable media shall be managed according to the robustness rules of Section 11.

10.4 Bound recording

10.4.1 Bound recording limited

When `digital_recording_control_data` of the digital copy control descriptor is set to '00', "copy free", content may be stored with no copy restrictions. When the `encryption_mode` of the content availability descriptor is set to '1', the content shall be protected as specified in Table 6.

When `digital_recording_control_data` of the digital copy control descriptor is set to '10'; "copy free in SD format and copy once in original resolution", the copy control information on the recordable media shall be set according to Table 6 for bound recording. Even when the content is bound recorded as '10', it is not necessary to change the value of the `digital_recording_control_data` on the digital copy control descriptor.

When the `digital_recording_control_data` on the digital copy control descriptor is set to '10'; "copy free in SD format and copy once in original resolution", multiple copies shall not be allowed. This does not apply to data storage for backup purposes in the area that is not accessible to users. The multiple copies restriction applies to each tuner unit. In the case of multiple tuner units, the multiple copies restriction is applied respectively. In standard resolution, there is no limit for the number of copies.

When the `digital_recording_control_data` on the digital copy control descriptor is set to '11'; "copy free of SD", the content in high-definition shall not be stored using different methods of the retention specified in 10.4.3.

10.4.2 No more copies

The contents bound recorded as "no more copies" shall not be copied. This does not apply to the move function specified in 10.4.4. Standard resolution copies may be copied freely.

To output the bound recorded content as "no more copies" to the high-speed digital interface, the "no more copies" protection of the DTCP shall be applied. More specifically, the `DTCP_CCI` of *DTCP_descriptor* shall be defined as "no more copies" and the content shall be encrypted for output.

Regarding the video and audio outputs, the same process as the `digital_recording_control_data` is set to '11' ("copy free in SD format") shall be applied, as specified in 8.4.2.

10.4.3 Retention

When the `digital_recording_control_data` on the digital copy control descriptor is set to '11' ; "copy free in SD format", content may be retained up to the maximum time allowed for retention.

When the retention time exceeds the maximum time allowed for retention, the contents shall be removed. The content shall be removed 5 minutes after the maximum time allowed for retention. Even when there are conditions that do not allow for accurate time control, like when the power supply to the receiver units is accidentally interrupted, the content shall be made unusable within an appropriate time period.

For the output of the retained content, the content shall be encrypted and transmitted as “no more high-resolution copies”. When output is made through the high-speed digital interface, the “non-retention-mode” specified by the DTCP shall be applied.

In terms of audio and video output, the same process used in the `digital_recording_control_data`, defined as ‘11’ (“free copy in SD”), shall be applied, according to 8.4.2.

10.4.4 Move function

If the copy control information after the bound recording is set to “no more copies”, the content may be moved according to the following conditions:

- the bound recorded content may be moved only to a single built-in recordable media or a digitally connected single recordable media. The move function shall not be used unless output to single recordable media is assured;
- while a move is in progress, it shall be ensured that the contents exceeding 1 minute cannot be played back simultaneously in both the source and destination of the move;
- after a move is completed, it shall be ensured that the contents that can be used are not present simultaneously in both the source and destination of the move. After a move is completed, the contents in the source of the move function shall be made unusable.
- regarding the output to a different place from the destination of the move function during a move operation, the protection interface rules, described in this standard under Sections 7, 8, 9 and 11 shall apply.

10.5 Digital recording with the removable recordable media

To receive the content of the digital television service, special video service, data service, special data service and bookmark of data service list, which are copyright-protected by the digital copy control descriptor and content availability descriptor, and to digitally record these contents to the removable recordable media, the recording formats and content protection systems for recording described in ARIB TR-B14:2006, Volume 8, Annex B shall be implemented, excluding the one related to the reception of one-seg services.

When the `digital_recording_control_data` on the digital copy control descriptor is set ‘10’; “copy free in SD format and copy once in original resolution”, multiple copies in high definition format are not allowed. This does not apply to digital recording for backup purposes in the area that is not accessible to end users. The recording restriction to the digital recordable media applies to each of the tuner units. In the case of multiple tuner units, the multiple copy restriction applies to each tuner unit respectively.

When the receiver units include a recording system that is incompatible with the `encryption_mode`, the contents which are copyright-protected by `copy_control_type` and `digital_recording_control_data` of the digital copy control descriptor, set to ‘01’ and ‘00’, respectively, and the `encryption_mode` of the content availability descriptor, set to ‘0’, may be digitally recorded by the recorder in the same way as the “copy free in SD format and copy once in original resolution”.

The contents that are not copyright-protected by the digital copy control descriptor and content availability descriptor may be, in principle, digitally recorded in any format. If necessary, the conditions applied to the removable recordable media, listed in ARIB TR-B14:2006, Volume 8, Annex B, excluding the one related to the one-seg services, shall apply.

10.6 Analog recording with the removable recordable media

High resolution analog recording can be carried out while the APS_control_data for the digital copy control descriptor is defined as '00' and the digital_recording_control_data is also set at '00'. When the APS_control_data is different to '00', the analog copy can only be made in standard resolution according to Table 3.

To make a recording from the content analog interface of the digital television service, the special video service, data service, special data service and bookmark of data service list for removable recording media, when the digital copy control descriptor indicates a configuration other than "free to copy", it shall be ensured that the content is not recorded in high resolution for removable recording media or, if recorded, suitable viewing is not made available during reproduction.

To make a recording from the content analog interface of the digital television service, the special video service, data service, special data service and bookmark of data service list for removable recording media, when the digital copy control descriptor indicates a "free copy" configuration, the content maybe recorded to the removable recording media without restriction.

11 Robustness rules for the receiver units

11.1 Basic requirements of robustness rules

Receiver units shall be designed and manufactured in such a way that the content protection function including output control and copy control, specified as part of the compliance rules described in Section 9, can not be undermined easily. The hardware and software shall not deliberately allow the bypassing of content protection mechanisms.

Receiver units shall be designed and manufactured in such a way that no piece of confidential information, including cryptographic algorithms used to protect the received contents, can be extracted in a usable manner.

11.2 Implementation methods of robustness

11.2.1 General aspects

The receiver shall not incorporate the functions that enable the easy undermining or bypassing of the contents protection function, modification or copying of contents in compressed digital signal format, or control signals, under protection. The examples are as follows:

- a switch, jumper or similar function that enables the bypassing of the protection function;
- specific wiring (which involves breaking and connecting) that enables the undermining of the protection function;
- functions such as service menu or remote control to test the protection function or output control, which allow the supervision of the protection function or output control.

11.2.2 Content output

The output of the content under protection is allowed according to Section 10.

The content encrypted using the local encryption method specified in 11.2.3.6 may be formatted in the compressed digital signal form to the output bus, accessible to the user.

11.2.3 Storing contents

11.2.3.1 General aspects

Protected items can only be stored in recordable media if they are encrypted using the local encryption method described in 11.2.3.6, or are protected through a method that prevents the illegal extraction or copy by the end user.

11.2.3.2 Prohibited reutilization of the copy

It shall be ensured that a content, which is copied from the storage, even in bit-by-bit form, cannot be reutilized (see 11.5).

11.2.3.3 Timer management for retention

The timer function for retention shall have 5 min precision and shall have the access protected from the user.

11.2.3.4 Management of other information

The information of copy and utilization restrictions generated from the information stored on the recording media, encryption or other similar methods, shall be applied to protect from any modification by end users. Information contained in the digital copy control descriptor, the content availability descriptor or information stored on the recording media is considered as restricted copy and use information.

11.2.3.5 Restrictions regarding internet re-transmission

All output interfaces that can be used for the retransmission of the signal via internet shall implement all the rules to protect the content, as specified in 10.3, according to Table 6.

11.2.3.6 Strength of local encryption

The local encryption shall be equal or stronger than common key symmetric encryption with at least a 100-bit long key.

11.2.3.7 Key management

The keys used for content encryption shall not be extracted from the receiver unit or user accessible bus, or stored in the recording media, without protection.

Secure key management such as the use of unique receiver key, or exclusive information of the receiver derived from the key, shall be used, in order to ensure that the playback of the content is disabled, when the recording media is connected to other receiver units, or other equipment, or when contents are illegally copied onto the recording media of another equipment.

11.3 User accessible bus

When data flows, specifically video *transport streams* and *elementary streams*, which are copy-protected (digital copies control descriptor containing *digital_recording_control_data* informing a different control from that of “free to copy”) are transmitted to any user-accessible local bus, they must be encoded using the local cryptography method. Alternatively, similar protection methods can be applied before the output.

A user accessible bus needed for protection means a digitally connected interface bus from which users can easily access signals, such as the PCI bus, USB bus, IDE bus, SCSI bus and PCMCIA interface bus that has standard sockets whose specifications are made publicly available.

A user accessible bus does not include memory buses, CPU buses and other buses that are difficult to access by end users.

11.4 Prohibition re-using of copies

Any bound recorded content that is encrypted by the local encryption method cannot be used on any other equipment even if the content is copied bit-by-bit. Appropriate implementation to disable the re-use of copies shall be made to prevent illegal actions.

The illegal generation of various copies shall be prevented by moving the contents from the copy source, after they are copied, onto another recording media and then returning the content copied to where they were originally located, and moving the content once again.

11.5 Actions that shall be prohibited regarding information control

Users shall be prevented from changing copy flags in order to enable copying, or changing the restrictions flags to enable unconditional copying. The actions that shall be prohibited to prevent users from adding modifications, include the modification of digital_recording_control_data in the digital copy control descriptor and the copy control information in the DTCP_descriptor, and the copy control information on the recording media.

11.6 Digital recording of contents to the removable recording media

The digital recording of content to the removable recording media shall comply with the criteria defined in items 11.1 to 11.5.

12 Output interface

12.1 Analog video output interface

The analog video component interface shall be bound to standard definition when the analog copy control is not "copy free", i.e., when the APS_control_data of the digital copy control descriptor is not set to '00'.

12.2 Digital video output interface

When outputting a digital video, the specifications in the HDCP shall apply.

The digital video output resolution shall be bound to standard definition when the HDCP authentication is not successfully executed and the digital copy control is not "copy free", i.e., when the APS_control_data of the digital copy control descriptor is not set to '00'.

12.3 Analog audio output interface

Analog audio can be output without protection.

12.4 Digital audio output interface

When outputting a digital audio, the specifications in the SCMS do not need to be applied to the SPDIF, however, the specifications of the HDCP protocol shall be applied to HDMI audio outputs.

12.5 Other digital output interfaces

When exporting content with an IP interface, firewire or USB, the specifications of protection in the DTCP shall apply.

Bibliography

- [1] ARIB STD-B10:2006, *Service information for digital broadcasting systems*
- [2] ARIB STD-B25:2006, *Conditional access system specifications for digital broadcasting*
- [3] IEC 61119:1992, *Digital audio tape cassette system (DAT)*