Digital terrestrial television broadcasting - Security Issues

Televisão digital terrestre – Tópicos de segurança – Parte 1: Controle de cópias

Televisión digital terrestre — Topicos de seguranca – Parte 1: Controle de reproduction

Digital terrestrial television broadcasting - Security Issues – Part 1: Copy control

デジタル放送におけるコンテンツ保護、第１部　デジタルコピー制御

Conditional access system specifications for digital broadcasting

Foreword

This document is the result of the joint efforts of the ABNT, ARIB and SBTVD Forum under the standardization and technical cooperation activities of the Brazil-Japan Digital Television Joint Working Group.

The Brazilian Association for Standardization (ABNT) is the organism responsible for technical standardization in Brazil, providing essential support for Brazilian technical development. It is private, non-profit organization, recognized as the only National Standardization Body. It provides Brazilian society with systematic knowledge, through normative documents, enabling the production, commercialization and use of goods and services, in a competitive and sustainable manner, in the internal and external markets, contributing to scientific and technological development, environmental protection and consumer's protection.

The Association of Radio Industries and Businesses (ARIB) was designated as "the Center for Promotion of Efficient Use of the Radio Spectrum" and "the Designated Frequency Change Support Agency" by the Minister of Internal Affairs and Communications (MIC) of Japan under the provisions of the Radio Law. Under this designation, ARIB conducts studies and R&D, establishes standards, provides consultation services for radio spectrum coordination, cooperates with other overseas organizations and provides frequency change support services for the smooth introduction of digital terrestrial television broadcasting. These activities are carried out in cooperation with and/or participation by telecommunication operators, broadcasters, radio equipment manufacturers and related organizations as well as under the support by MIC.

The Brazilian Digital Terrestrial Television Forum (SBTVD Forum) is a non-profit entity, created with the objective of aiding and stimulating the development and implementation of best practices aiming at the success of systems reality for digital broadcasting of images and sounds in Brazil. Since the creation of the SBTVD Forum in February, 2007, its members have endeavored to establish standards of technical quality which permit deployment of digital television in Brazil. The Technical Module has contributed to the preparation of standards, with active participation by universities, research centers, related industry organizations and broadcasters.

This document does not describe the industrial property rights mandatory to these standards.

This document has no standardization value. Its purpose is to serve as a reference for characterizing the specificities of Brazilian and Japanese digital terrestrial television standards within the scope of the Brazil-Japan Digital Television Joint Working Group.

This document is drafted in accordance with the rules established in the ISO/IEC Directives, Part 2.

In the Brazilian and Japanese harmonized documents, commonalities are described in Clause 5 where Table 1 includes all references to ABNT and ARIB related documents. Differences are described in Clause 6. In each subclause, a reference to the corresponding Brazilian and Japanese related session is included in separate boxes in *italic text*.

No reference is made to the domestic policies of the countries.

1 Scope

This document characterizes the copy protection mechanisms for digital terrestrial television broadcasting in Brazil and Japan.

2 Normative references

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

ARIB TR-B14:V6.2 Vol.4:2016, *Operational Guidelines for Digital Terrestrial Television Broadcasting: Provision for PSI/SI Operation*

ARIB TR-B14:V6.2 Vol.8:2016, *Operational Guidelines for Digital Terrestrial Television Broadcasting: Provision for Contents Protection*

ARIB STD-B25:V6.5:2015, *Conditional Access System Specifications for Digital Broadcasting: Reception Control System (Conditional Access System)*

ABNT NBR 15605-1:2008, *Digital terrestrial television broadcasting – Security Issues – Part 1: Copy control*

3 Terms and definitions

For the purposes of this document, the abbreviated terms given in ABNT NBR 15605-1 and ARIB TR-B14 Vol.4 and ARIB TR-B14 Vol.8 the following apply.

Bound Recording	Bound Recording is defined as the recording function to enable recorded content to reproduce only on the equipment that has recorded the content.
Free program	A program which is not chargeable and. is described as free_CA_mode=0 in SDT and EIT.
Pay program	A program which is chargeable and is described free_CA_mode=1 in SDT and EIT.
Content protection system	The contents protection system is defined as the technique that uses, for example, encryption, to prevent the illegal modification and copying of contents, for the purpose of protecting the rights on contents.

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ABNT NBR 15605-1, ARIB TR-B14 Vol.4 and ARIB TR-B14 Vol.8, 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
SDT	Service Description Table
TS	Transport Stream
USB	Universal Serial Bus

5 Commonalities of the content protection systems

The common parts of ABNT NBR 15605-1, ARIB TR-B14 Vol.4 and ARIB TR-B14 Vol.8 and its correspondence are described in Table 1.

Table 1 — Correspondence between ABNT NBR 15605-1 and ARIB standards

Description	ABNT NBR reference clause	ARIB TR-14 reference clause Volume 8	ARIB TR-14 reference clause Volume 4
Copy control general rules	5	4.1	21.1
Services type	6	4.4 Also described in ARIB TR-14 Volume 5.4.4.1	8.1 Also described in ARIB TR-14 Volume 2 7.10
Digital copy control descriptor and content availability descriptor	7.1	4.1.2	21
Default values for copy control	7.3	NA	21.2
Descriptors	8.1	4.1	30.3.2.2
Copy control information operational rules	8.2	4.1	21 and 30.3.3.3
Copy control for data services	8.3	4.1.2	30.3.3.3
Category 1: Copy free	8.4.1	5.5.1, 5.3.2 and 5.3.3	21
Maximum bit rate value definition	9.1.1	3	21.3
Maximum bit rate default value	9.1.2	3	21.3.1
Maximum bit rate for multicamera	9.1.3	NA	21.3.2
Default copy control rules	9.3.1	NA	21.5.1
Encryption Plus Non-Assertion (EPN)	9.3.2	5.3.3	21.5.2
Content retention mode	9.4	NA	21.6
Full-seg rules overview	10.1	Part1 5	NA
Output rules with the encryption plus non-assertion bit	10.2.3	5.3.3	21.5.2
Internet retransmission rules	10.3	5.4	NA
Bound recording	10.4.1	5.5.1	NA
No more copies in high definition	10.4.2	5.5.2	30.3.2.2
Move function	10.4.4	5.5.4	NA
Digital recording with the removal recordable media	10.5	5.6	NA
Analog recording on removable media	10.6	5.7	NA
Robustness rules	11.1	6.1	NA
Robustness rules implementation overview	11.2.1	6.2.1	NA
Content output	11.2.2	6.2.2	NA
Content storing overview	11.2.3.1	6.2.3	NA
Prohibition of re-use of the copy	11.2.3.2	6.2.3.1	NA
Time precision to bounded copy	11.2.3.3	Part1 6.2.3.2	NA
Other Information Management	11.2.3.4	6.2.3.3	NA

Internet retransmission restrictions	11.2.3.5	5.4 and 7.3	NA
Keys management	11.2.3.7	6.2.4.2	NA
User accessible data bus	11.3	7.5	NA
Prohibition of re-use of the copy	11.4	7.6	NA
Not allowed actions to information control	11.5	7.7	NA
Digital recording on removable media	11.6	7.8	NA
Digital video output	12.2	5.3	21
Digital audio output	12.4	5.3	21
Other digital interfaces	12.5	5.3	NA
* Items identified with the letters “NA” represent those not directly addressed by the particular technical document.			

Referenced items of Table 1 are a general correlation of the subjects in all issues listed in the description column on both ARIB and ABNT standards. However, the same topics can be addressed in additional portions of the technical documentation, either as sparse paragraphs, references or footnotes.

6 Differences of the content protection systems

Table 2 — Differences between ABNT NBR 15605-1 and ARIB standards

Description	ABNT NBR reference clause	ARIB TR-14 reference clause Volume 8	ARIB TR-14 reference clause Volume 4
Copy control information priorities	7.2	4.1.2	21.1
Default values for copy control	7.3	NA	21.2
Copy control categories	8.4	NA	NA
Category 2: Copy free in SD	8.4.2	NA	NA
Category 3: Copy free in SD and copy once in HD	8.4.3	NA	NA
Changes on copy control information	9.2	NA	21.4
Default copy control rules	9.3.1	NA	21.5.1
Output requirements	10.2.1	5.3.1	21 and 21.1
Output rules by Digital Copy Control Descriptor and Content Availability Descriptor	10.2.2	5.3.2	30.3.2.2
Retention	10.4.3	5.5.3	21.6
Local cryptography strength	11.2.3.6	6.2.4.1	NA
Analog video output	12.1	5.3	30.3.2.2
Analog audio output	12.3	5.3	30.3.2.2
Items identified with the letters “NA” represent those not directly addressed by the particular technical document.			

*

Referenced items of Table 2 present practical differences in the topics defined at the description column on both ARIB and ABNT standards. However, the same topics can be addressed in additional portions of the technical documentation, either as sparse paragraphs, references or footnotes.

6.1 Access control systems

Content protection system in ARIB standards utilizes an access control system for use in digital broadcasting, defining scrambling and associated information specifications as well as related reception specifications for a system that provides control during signal reception ("conditional access system"). Detailed information on this system can be found on ARIB STD-B25.

No similar access control system or encryption mechanism related reception specifications is described on ABNT's standards for content protection, and, therefore, no provisions for such feature are described in ABNT NBR 15605-1.

This difference will also marginally impact other issues of the systems such as: "Changes on copy control information" and "Full-seg rules overview". It's important to say that both ABNT and ARIB standards are very similar in those aspects, and that any deriving issue that relates to access control systems related to reception specifications are presented in the list below for the sake of simplicity.

6.2 Copy free in Standard Definition

ABNT NBR 15605-1 in item 8.4.2 determines that, whenever the copy control information of standard definition is received, the content resolution exported through the analog interface shall be equivalent to standard definition. For digital video outputs, when the digital copy control information is received, the result of the authentication protocol shall be verified. If authentication of digital outputs fails content should be converted to SD resolution. ARIB standards include protection mechanisms for the analog output of SD video and HD video, with the use of available Macrovision copy protection technology, as described in Clause 4 of ARIB TR B14 Vol. 8. No such provision is included in ABNT the documents. Analog video outputs mechanisms, although majorly similar, are also marginally affected by this difference.

Additionally, copy control references in the ARIB standard for analog outputs that apply the "*Copy never*" process to CGMS-A and SCMS, or Macrovision *APS_control_data* is set to other than "00", will be equivalent as the "Copy free in SD format" category in ABNT documents.

6.3 Copy control categories

Subclause 8.4 of ABNT NBR 15605-1 defines categories for copy control differently than ARIB TR B14 Vol. **8** subclause 4.1.2. ABNT's standards address copy control categories from the perspective of video resolution made available at the receivers outputs. ARIB documents describes protection mechanisms based on copy control signalization does not necessarily relates to video resolution at the receivers output.

ABNT NBR 15605-1 describe only three categories for copy control in: item 8.4.1 (Category 1: "*copy free*"); item 8.4.2 (Category 2: "*copy free in SD format*"); and item 8.4.3 (Category 3: "*copy free in SD format and copy once in original resolution*").

6.4 Services type

Clause 6 of ABNT NBR 15605-1 is based on ARIB TR B14 Volume 4 subclause 8.1. It contains the digital television services type description. Although there are major similarities on the use of service-type information between the two systems, the use of some of them are different, particularly regarding testing and special video services.

In the Brazilian digital terrestrial television system, according to ABNT NBR 15605-1, Clause 6:

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, 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

6.5 Copy control information priorities

Clause 7.2 of ABNT NBR 15605-1 is based on ARIB TR B14 Volume 4 subclause 21.1. It contains the digital television services type description.

In the Brazilian digital terrestrial television system, according to ABNT NBR 15605-1, Subclause 7.2:

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.

In the Japanese digital terrestrial television system, according to ARIB TR B14 Volume 4, Subclause 21.1:

Copy control information in a Digital Copy Control Descriptor placed in the PMT is used when a program is actually recorded, and copy control information described in the EIT is used when preparing for the start of recording. Please note that when there is no descriptor in the EIT and when there is in the SDT, the description in the SDT should be used.
When descriptors are present in the first and second loops of the PMT, the description in the second loop should be given a priority for the relevant component. However, the copy control information described in the second loop becomes valid only for components whose "component_tag" is set to a value between '0x40' and '0x7F' (See Section 30.3.3.3). When a descriptor is present in the second loop for a component with other values (for example, when the maximum bit rate of a video component needs to be specified), the description of the first loop is given a priority (when there is no descriptor in the first loop, the default copy control information is applied).
Additionally, for the control of analogue video output, digital audio output and output of IEC60958 conformant audio streams from a high-speed digital interface, the description of the descriptor in the first loop of the PMT should be given a priority. For the control of MPEG TS output from a high-speed digital interface, the description of a component with the most strict copy control among components to be output (when specific components are deleted from received services, remaining components after the deletion) should be given a priority. See the section of Digital Copy Control Descriptor for concrete levels of copy control.
The real recording control is definitely performed based on the description in the PMT. When non-default copy control (see next section) is performed, a descriptor should be present also in the PMT.
Information of Digital Copy Control Descriptors in the SDT and EIT is used when a setting of recording schedule. To

specify information on copy control regarding a whole service, a Digital Copy Control Descriptor should be present in the SDT. To specify information regarding copy control specific to each event, a Digital Copy Control Descriptor should be present in the EIT. When Digital Copy Control Descriptors are present in both SDT and EIT, the description in the EIT should be given a priority.

6.6 Default values for copy control

Subclause 7.3 of ABNT NBR 15605-1 is based on ARIB TR B14 Volume 4 subclause 21.2. It contains the digital television services type description.

In the Brazilian digital terrestrial television system, according to ABNT NBR 15605-1, Subclause 7.3:

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 Japanese digital terrestrial television system, according to ARIB TR B14 Volume 4, Subclause 21.2:

The default digital copy control information, when a Digital Copy Control Descriptor is not present in either of PMT, SDT or EIT, is "Copy freely". Specifically, this is equivalent to
(a) For a digital TV service and special video service, copy_control_type='01', digital_recording_control_data='00'
(b) For a data service transmitted in a layer other than the partial reception layer and special data service copy_control_type='01/11', digital_recording_control_data='00'
(c) For a data service transmitted in the partial reception layer copy_control_type='10', digital_recording_control_data='00'
As described above, as the final recording control is performed in accordance with the description in the PMT, no matter what sort of digital copy control information is in the EIT and SDT, as long as this descriptor specified as other than "Copy freely" is not present in the PMT, the final control will be "Copy freely", which should be kept in mind. However, as the basic rule, there should not be any inconsistency between information in the SI (SDT and EIT) and PSI (PMT).

6.7 Output rules by Digital Copy Control Descriptor and Content Availability Descriptor

Subclause 10.2.2 of ABNT NBR 15605-1 defines rules for digital copy control with minor changes when compared to ARIB TR B14 Vol. 8 subclause 5.3.2. Nevertheless, the overall copy control behaviours and signalization is generally the same.

However, ABNT's standard does not include High-Speed Digital Interface (Serial Interface) IEC60958 as one of the possible interfaces subjected to copy control. Also, there's no copy control requirement on the ABNT's standard for Analog Video Outputs or Digital Audio Outputs.

6.8 Local cryptographic strength

There are differences in the common key symmetric encryption length between ABNT NBR 15605-1 and ARIB TR B14 Vol. 8.

In the Brazilian digital terrestrial television system, according to ABNT NBR 15605-1, Subclause 11.2.3.6:

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

In the Japanese digital terrestrial television system, according to ARIB TR B14 Volume 8, Subclause 6.2.4.1:

Local encryption shall be equal or stronger than common key encryption with a 56-bit long key, and use cryptographic algorithms (for example, DES) that can guarantee sufficient safety.