

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 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.

© ITU 2006

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	1
3	Terms and definitions	1
4	Abbreviations, acronyms and conventions	3
5	Overview	4
5.1	Key goals	4
5.2	Key features.....	4
5.3	Key technical points	4
5.4	DRM bridge general requirements	5
5.5	Background.....	5
6	Robustness requirements	6
6.1	Construction	6
6.2	Controlled content paths.....	7
6.3	Methods of making functions robust.....	7
7	Compliance rules	8
7.1	Introduction	8
7.2	Outputs	9
7.3	Copying, recording, and storage of controlled content	9
8	Change control.....	11
Annex A	– Copy control information	12
A.1	Channel change	12
A.2	CCI Definition.....	12
A.3	EMI – digital copy control bits.....	12
A.4	APS – analogue protection system.....	13
A.5	CIT – constrained image trigger.....	13
A.6	Authenticated tunnel protocol	13
Annex B	– Robustness checklist.....	14
Appendix I	– Digital outputs.....	16
Appendix II	– Review criteria.....	17
II.1	Video transport	17
II.2	Security interfaces	17
II.3	Points of attack and system weaknesses.....	17
II.4	Effectiveness of proposed technology	18
II.5	Security processing.....	18
II.6	Revocation and renewability of keys	18

	Page
II.7 New algorithms	18
II.8 Preservation of service integrity	18
II.9 Licensing terms	19
II.10 Overall impact on the video distribution network.....	19
Appendix III – Elements of technology review submission	20
III.1 Licence terms.....	20
III.2 Security overview	20
III.3 Video transport	20
III.4 Content protection profiles	21
III.5 Key exchange algorithms	21
III.6 Security interfaces	21
III.7 Security processing.....	21
III.8 Certificate management.....	21
III.9 Revocation/renewability of key.....	22
III.10 Points of attack/potential weaknesses	22
III.11 Commercial use	22
III.12 Contact information.....	22

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