国 际 电 信 联 盟

ITU-T J.197

国际电信联盟
电信标准化部门

(11/2005)

J系列：有线网和电视、声音节目及其他多媒体信号的传输

有线调制解调器

从有线接入网到归属网的数字权利管理（DRM）网桥的高层需求

ITU-T J.197建议书

国际电信联盟

ITU-T J.197建议书

从有线接入网到归属网的数字权利管理（DRM）网桥的高层需求

摘　要

本建议书定义了从有线接入网到归属网的数字权利管理网桥的需求，网络运营商可以传送许多类型的内容（如视频、音频等）给它，并确保内容的使用方式不违反任何服务协议或法律要求。

来　源

ITU-T 第 9 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 11 月 29 日批准了 ITU-T J.197 建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

ITU-T J.197建议书

从有线接入网到归属网的数字权利管理（DRM）网桥的高层需求

1 范围

本建议书定义了从有线接入网到归属网的数字权利管理网桥的需求，网络运营商可以传送许多类型的内容（如视频、音频等）给它，并确保内容的使用方式不违反任何服务协议或法律要求。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

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

2.2 资料性参考文献

– 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 术语和定义

本建议书规定下列术语：

3.1 analogue protection system bits（APS bits） 模拟保护系统位（APS 位）：CCI 的第 3 位和第 2 位，用于指明机顶盒的模拟保护状态。

3.2 compliance rules 依从规则：适用于机顶盒的规则，目的是防止对受控内容进行未经授权的拷贝。

3.3 consensus watermark 一致认可的水印：一个用于 DRM 中的标准水印。

3.4 constrained image 受限的图像：相当于每帧不超过 520 000 像素的图像（例如，一幅分辨率为 540 垂直线、960 水平线的图像，其宽高比为 16：9）。受限的图像可以输出，或利用视频处理技术进行显示，如线加倍或锐化，以便改善图像的感知质量。

3.5 constrained image trigger（CIT） 受限的图像触发器（CIT）：在机顶盒高清晰度模拟输出中，用于触发“受限的图像”输出的字段或位。

3.6 content protection 内容保护：应用技术保护措施，防止对网络传送内容进行未经授权的复制与/或重新分配。

3.7 controlled content 受控内容：视频服务提供商网络传送的内容，其加密模式指示器（EMI）位设置成一个非（0，0）值，（0，0）表示“拷贝不受限”。

3.8 copy control information（CCI） 拷贝控制信息（CCI）：一个 1 字节的字段，机顶盒利用其包含的信息来控制内容的拷贝。更多信息参见附件 A。

3.9 digital rights management（DRM） 数字权利管理（DRM）：定义、管理和实施一系列内容使用规则。这些使用规则将指明诸如内容特定片断拷贝、查看或分配权利等事项。

3.10 digital transmission content protection（DTCP） 数字传输内容保护（DTCP）：在题为“5C 数字传输内容保护 1.0 版”规范中所述的加密、解密、密钥交换和可更新方法。

3.11 DRM bridge DRM 网桥：分配与投入使用归属网基础设施和技术，以便实现对内容的保护，以及对归属网上所保存和分配的网络传送内容的数字权利管理。

3.12 encryption mode indicator bits（EMI Bits） 加密模式指示器位（EMI 位）：与所保护内容相关的两个比特位，用于规定对相关内容允许进行的拷贝操作。

3.13 high definition analogue form or output 高清晰度模拟形式或输出：一种非数字形式的格式或输出，具有比标准清晰度模拟形式或输出更高的分辨率。

3.14 high-bandwidth digital content protection（HDCP） 高带宽数字内容保护（HDCP）：在题为“高带宽数字内容保护系统 1.0 版”规范中所述的认证、加密、解密和更新方法。

3.15 product 产品：一种设备与/或技术，它接收并可能分配内容，带有重新分配控制功能与/或拷贝控制功能。

3.16 robustness rules 稳健性规则：在第 6 条中所述的规则，适用于机顶盒，目的是抵御各种修改机顶盒以破坏依从规则的企图。

3.17 service 服务：通过视频服务提供商网络向（或自）机顶盒传送的、模拟或数字格式的视频、音频或数据信号，目的是实现对信息、娱乐或通信内容的接收或传输。

3.18 set top box（STB） 机顶盒（STB）：能直接从视频服务提供商处接收内容的任何设备，包括与显示设备分开的设备，以及具有适当的嵌入式功能的显示设备。STB 充当归属网服务网关的作用，并包括有条件的接入（CA）系统和数字权利管理（DRM）系统。

3.19 standard definition analogue form or output 标准清晰度模拟形式或输出：一种非数字形式的格式或输出（例如，PAL RF、NTSC RF、复合、S-视频、YUV、Y、R-Y、B-Y 或 RGB），具有不超过 483 行的隔行或逐行有效扫描线。

3.20 video content protection system（VCPS） 视频内容保护系统（VCPS）：用于记录 DVD+RW 和 DVD+R 光数字媒介上的加密内容，受 VCPS 技术保护。

3.21 video service provider（VSP） 视频服务提供商（VSP）：提供如本建议书中所述之“服务”的服务提供商。

4 缩写词、首字母缩写词和惯例

本建议书采用下列缩写：

AES	高级加密标准
APS	模拟保护系统
CCI	拷贝控制信息
CGMS-A	拷贝生成管理系统 — 模拟
CIT	受限的图像触发器
DRM	数字权利管理
DTCP	数字传输内容保护
DVD-RW	数字多功能盘 — 可重写
DVD+R	数字多功能盘 — 可记录
DOCSIS	经由有线服务接口规范的数据
DVI	数字视频接口
EEPROM	电可擦除可编程只读存储器
EMI	加密模式指示器
HDCP	高带宽数字内容保护
HDMI	高清晰度多媒体接口
IP	网际协议
LSB	最低有效位
MPEG	运动图像专家组
NTSC RF	国家电视系统委员会（制式） 射频
OOB	频带外
PAL	逐行倒相（制式）
PCI	外围部件接口
PCMCIA	个人计算机存储卡国际协会
QoS	服务质量
RF	射频
RGB	红、绿、蓝（三原色）
SRM	系统更新消息
STB	机顶盒
S-Video	超级视频
VCPS	视频内容保护系统
VSP	视频服务提供商
WTSA	世界电信标准化全会

5 概述

归属网技术及其对它的认同已发展到这样一个阶段，即归属网已成为一种引人注目的娱乐网络，允许用户在归属网所连接的各种设备间存储和分配内容。业界关注的是如何进一步发挥该环境的作用，将娱乐服务提供扩展至归属网。由于有线服务常常涉及到高质量的、受版权保护的内容，因此，出于众多法律和商业方面的原因，更加需要定义内容保护机制，应用相关的使用规则。本建议书确立了从有线接入网到归属网的数字权利管理（DRM）网桥的需求，网络运营商可以传送内容给它，并确保内容的使用方式不违反任何服务协议或法律要求。

5.1 主要目标

实施 DRM 网桥的目标包括以下内容：

- 从内容提供商角度来看的充分的稳健性。
- 从订户角度来看的非侵入性。
- 与监管和法律环境相协调。

5.2 主要特性

以下是 DRM 网桥的主要特性：

- 对参与传输与/或消费视频内容的所有设备进行认证。
- 对已建立的、作为 STB 一部分的数字权利管理内容保护商业规则（拷贝限制、播放次数、时间限度等）进行扩展和丰富。
- 所传输/消费的视频内容的加密/解密。

5.3 主要技术点

以下是 DRM 网桥的众多关键技术点：

- DRM 网桥将 DRM 的关键要素扩展到 STB 之外的点上。
- DRM 网桥既支持传输和存储有线运营商提交的内容，也支持传输和存储非有线运营商提交的内容。
- 带重新分配或拷贝控制功能的内容只能通过经批准的输出退出 STB 或下行流元素。
- 不带重新分配或拷贝控制功能的内容可以在 STB 或下行流元素内进行消费和存储。
- 不带重新分配或拷贝控制功能的内容可以自由地退出 STB 或下行流元素。

5.4 DRM 网桥一般要求

G-1	**subscriber-friendly 订户友好性：**DRM 网桥必须对订户透明，允许方便地进行内容消费，使用上没有障碍。
G-2	**simple usage model 简单使用模型：**DRM 网桥将采用简单使用模型，允许依据内容提供的权利，在归属网内使用所购买的网络运营商提供的内容。
G-3	**content protection 内容保护：**DRM 网桥必须防止未经授权的传输，并防止在归属网外拷贝受保护的内容。
G-4	**block theft-of-service 防止对服务的窃取：**DRM 网桥必须防止对服务的窃取，并保护内容使用规则（例如，在一个多处单元中窃取无线网络上的内容）。
G-5	**compatible with other DRM technologies 与其他 DRM 技术的兼容性：**对非有线运营商传送的内容，DRM 网桥不应排除使用其他内容保护技术。
G-6	**transport agnostic 传输无偏差：**用于实现 DRM 网桥的技术必须独立于归属网技术。
G-7	**backward compatible 向后兼容性：**DRM 网桥技术不得影响现有的视频分配业务。
G-8	**distribution agnostic 分配无偏差：**DRM 网桥务必支持各种不同的分配技术，包括 MPEG 广播、IP 流和 FTP。
G-9	**real time protection 实时保护：**用于实现 DRM 网桥的技术应适用于实时媒介（例如，广播 MPEG 和 IP 流源）。
G-10	**integrated 集成性：**DRM 网桥技术和处理应与其他相关的行业倡议，如 DOCSIS（ITU-T J.112/J.122 建议书）、IPCablecom（ITU-T J.16x 和 J.17x 系列建议书）和 IPCable2Home（ITU-T J.19x 系列建议书）兼容。
G-11	**open specification 开放性：**DRM 网桥规范应使各种不同供应商设备间能够实现互操作。
G-12	**economically feasible 经济可行性：**DRM 网桥技术和处理的实现、维护、验证和实施必须支持合适的商业模型。
G-13	**dynamically manageable 动态管理性：**用于保护内容的信息必须是动态可配置和可管理的。
G-14	**renewability 可更新：**DRM 网桥安全性软件必须是可更新的。
G-15	**functional during outage 中断期间的功能发挥：**当接入有条件的接入系统遭到损坏时，应支持向归属网分配受控和非受控内容。
G-16	**unprotected content 未受保护的内容：**DRM 网桥对非保护内容的使用应没有任何影响。
G-17	**extent of content protection 内容保护的范畴：**对归属网上的所有视频传输，都应具备内容保护功能，它由 DRM 规则集建立。
G-18	**DRM rule set extension DRM 规则集扩展：**DRM 中提供了丰富的 DRM 规则集（拷贝、重播、查看时间等），务必由 STB 进行管理，并扩展至下行流元素。
G-19	**client authentication 客户认证：**对归属网连接的、涉及视频内容传输与/或消费的所有元素，都应支持认证。
G-20	**encryption 加密：**对归属网内的视频传输，必须提供内容加密功能。
G-21	**device revocation 设备撤回：**应提供具备拒绝内容接入某个特定设备的能力，即使该设备在某个时刻是一个合法的 DRM 网桥网络元素。

5.5 背景

当涉及经由安全分配网络传送受保护内容时，有一点至关重要，即用于保护内容免受未经授权拷贝或重新分配的技术应是可用的。另外，设备本身必须足够稳健，能够抵御安全风险。本建议书详细阐述了内容保护技术的要求、稳健性以及用于处理受保护内容的设备的依从要求。这些内容技术和稳健性要求是从客户接收设备（即机顶盒）的角度进行描述的，机顶盒接收来自视频服务提供商的内容，作为有线分配网络的一部分，它必须为高价值内容提供保护。内容在源头进行加密，在穿过服务提供商网络时受到保护。本建议书的目的是确保一个在归属网中可用的安全性比较等级。通过桥接，以一种稳健、安全的方式，将内容流入下行流环境，是本建议书所关注的主要问题。

允许服务提供商内容退出机顶盒的内容保护和数字输出技术务必确保服务提供商继续保持对该内容拷贝和重新分配的控制，即使是在内容退出机顶盒而转入其他设备后。包含任何数字输出、DRM 或内容保护技术的机顶盒设备下行流还必须满足本建议书为机顶盒确立的稳健性和依从规则要求。为机顶盒确立的稳健性和依从规则用于控制总的下行流生态系统。

6 稳健性要求

接收并可能分配受保护内容的设备必须满足众多的稳健性要求，以便确保为内容提供充分的保护。已经认识到稳健性可能因设备可用的内容不同而不同，稳健性可能需要随安全技术的变化而随时变化，需要积极应对这种技术变化。本节描述一个建议的、一般性的设备稳健性要求集。

6.1 构建

6.1.1 概述

产品必须满足依从规则要求，并以如下方式进行设计和制造，即能够有效挫败各种修改机顶盒以破坏依从规则的企图。

6.1.2 废除的功能

产品不得包括：

i） 开关、按钮、跳线、能被切断的特殊痕迹，或相当于前述内容的软件；或

ii） 服务菜单或功能（包括遥控功能）；

每种情况下，利用这些可以破坏内容保护技术、模拟保护系统、再保护措施、输出限制、记录限制或依从规则的其他强制性规定，或者利用这些可以将受控内容透露给未经授权的拷贝。就本建议书而言，“再保护措施”指的是：需要时，应用一种经过批准的保护技术，对接收自视频分配网络的内容实施控制，这些内容来自机顶盒的输出，利用这些保护技术，系统和方法的完整性得以保证。

6.1.3 保密

为了挫败未经授权各方对安全性的破坏企图，产品必须以如下方式进行设计和制造，即能够有效挫败发现或泄漏以下内容的企图：

i） 分配给每个机顶盒的特定比特长度的惟一号码，或者受控内容加密或解密处理中使用的各号码（统称为“密钥”）；以及

ii） 用于产生此类密钥的方法和密码算法。

6.2 受控内容路径

除了在依从规则和产品中所规定的输出外，在其他输出中内容不可用，受控内容不得以非加密、压缩形式出现在任何用户可达的总线上（如下定义）。同样，在产品数据中用于支持任何内容加密与/或解密的未加密密钥不得出现在任何用户可达的总线上。“用户可达的总线”指的是为最终用户升级或接入而设计的数据总线，如有插槽的 PCI（或用户可达的其他机制）、SmartCard、PCMCIA 或 Cardbus。

6.3 使功能变得稳健的方法

产品必须至少使用以下技术来增强本建议书中所述的功能和保护。

6.3.1 分配功能

产品中执行认证和解密的部分以及 MPEG（或类似的）解码器必须以如下方式进行设计和制造，即相互之间应该关联或能够实现集成，从而使在产品这些部分间以任何可用形式流动的受控内容对第 6.3.5 节中所述的保护等级而言必须是安全的，以免受截获或拷贝。

6.3.2 软件

以软件形式实现部分内容保护技术的产品的任何部分必须包括第 6.1 节和第 6.2 节中所述的所有特性。就本建议书而言，“软件”指的是一种功能实现形式，它依据本建议书确立的要求、利用指令或数据组成的计算机程序代码进行实现，此处的指令或数据指的不是硬件中所含的指令或数据。这种实现必须：

a） 通过任何合理的方法，使之符合第 6.1.3 节的要求，包括但不限于加密、以环 0 或超级用户模式执行部分实施方案，与/或在一个安全、物理的实施方案中体现，并且对软件的每种实施方案，应使用有效的伪装技术进行伪装，阻碍任何试图探寻所用方法的企图。

b） 在设计上具有对其组成部件进行自检的功能，这样，未经授权的更改在实施过程中将产生一个故障信息，提供给授权的认证与/或解密功能。出于本规定的目的，更改包括对第 6.1 节和第 6.2 节相关的特征或特性所做的任何修改、干扰或侵入，或对第 6.1 节和第 6.2 节相关的处理的任何中断。本规定要求至少对码进行循环冗余校验，这是利用专用密钥或安全散列算法所做的进一步加密。

c） 满足第 6.3.5 节所述的保护等级。

d） 在设计上提供保护机制，使之免受未经授权软件的攻击。

6.3.3 硬件

以硬件形式实现本建议书要求的产品的任何部分必须包括第 6.1 节和第 6.2 节中所述的所有特性。出于这些稳健性规则的目的，“硬件”指的是一个物理设备，包括某个组成部件，它实现某个内容保护要求，该要求是本建议书要求产品遵守的，并且：

i） 除了永久嵌入此类设备或部件中的指令或数据，不包括任何其他指令或数据；或

ii） 包括不永久嵌入此类设备或部件中的指令或数据，这些指令或数据是为此类产品或部件定制的，并且最终用户无法通过产品或部件访问这些指令或数据。

这种实现必须：

a） 通过任何合理的方法，使之符合第 6.1.3 节的要求，包括但不限于在无法适当读取的集成电路或固件中嵌入密钥、密钥生成方法和密码算法加密，或在上面软件相关章节中所述的技术；

b） 在设计上使得任何危及所评估技术或机顶盒安全或内容保护特性的、以某种方式进行再编程、移去或替换硬件元素的企图，都将带来严重的风险，将造成产品的损坏，使之无法再对受控内容（一个连接而非“套接”的部件）进行接收、解密或解码；

c） 满足第 6.3.5 节所述的保护等级。

6.3.4 混合

设计的产品硬件部分与软件部分之间的接口应提供上述纯硬件或纯软件实施方案所能提供的保护等级类似的保护等级。

6.3.5 保护级

必须依据 FIPS 140-2 “密码模块的安全性要求”“等级 2”实施核心加密功能（维护密钥、密钥生成方法和密码算法的机密性，符合依从规则的要求，防止已解密的受控内容被拷贝或被未经授权地查看），至少，它们应以某种方式保证：

a） 可以合理地预见，无法只用一般目的的工具或设备就能将它们挫败或欺骗，这些工具或设备用适当的价格即可广泛获得，如螺丝刀、跳线、夹子、电烙铁（“广泛可获得的工具”），或用适当的价格即可广泛获得的专用电子工具或专用软件工具，如 EEPROM 读写器、调试器或反编译器或类似的软件开发工具（“专用工具”），这些设备或技术不是为回避或欺骗要求的保护技术这一特殊目的而专门设计和获得的（“欺骗设备”）；以及

b） 只有使用专业的工具或设备才能困难地将它们挫败或欺骗（只有依据不透露协议才能获得的欺骗设备和专业工具或设备除外），如逻辑分析仪、芯片分解系统、在线模拟器或其他工具、设备、方法或技术，它们不包括在上面定义的、广泛可得的工具和专用工具内。

7 依从规则

7.1 引言

为了能被接受并附加于视频服务提供商的网络上，用于接收受保护的内容，设备务必符合众多条件要求。

7.2 输出

7.2.1 概述

产品不得输出内容或将接收到的内容通过服务传送给本建议书允许之外的任何输出。就本建议书而言，认为一个输出必须包括但不限于任何内部拷贝、记录或存储设备的任何传输，但不包括以其他方式满足这些依从规则和稳健性规则要求的内部非永久或暂时的传输。

7.2.2 标准清晰度模拟输出

如果内容依据适当的、有关模拟内容拷贝保护的国家或区域标准得到了适当保护，那么带任何标准清晰度模拟输出的产品只能通过服务输出接收到的内容，或通过服务传送接收到的输出。

7.2.3 高清晰度模拟输出

当 CIT CCI 位要求时，产品必须能限制内容的分辨率为高清晰度，它将通过能够以高清晰度模拟形式传输内容的连接输出。产品必须包括一个或多个经批准的数字输出。所有产品都必须生成和传播针对所有高清晰度模拟输出的 CGMS-A 信号；不过，除非适当的法律或规则要求，否则不得考虑 CGMS-A 触发器。

7.2.4 数字输出

带数字输出的产品只能通过服务输出接收到的内容，或通过本建议书允许的服务传送接收到的输出。在附录 I 中包含了一个经过测试、符合本建议书要求的技术清单。

7.2.5 不受水印干扰

产品和部件不得剥去、模糊或干扰已解密受控内容中的、一致认可的水印。

7.3 受控内容的拷贝、记录和保存

7.3.1 概述

除非本节允许，否则产品（无限制地包括具有内在或集成拷贝、记录或存储功能的产品）不得拷贝、记录或存储受控内容。

7.3.2 仅用于显示的缓冲区

只有出于使之能够立即显示受控内容这一目的，产品才能临时存储受控内容，前提是：

a） 内容显示后，存储的内容不再存在；以及

b） 数据不得以如下方式进行存储，即能够支持针对其他目的的拷贝、记录或存储。

7.3.3 不得拷贝多次

产品不得拷贝、记录或存储如下受控内容，即在 EMI 位中已指定内容已经拷贝并不得多次拷贝（“不得拷贝多次”），除非第 7.3.2 节或第 7.3.5.2 节允许。

7.3.4 决不得拷贝

除非第 7.3.2 节或以下内容允许，否则产品（无限制地包括具有集成记录功能的产品，如所谓的“个人视频记录仪”）不得拷贝在 EMI 位中已指定决不得拷贝（“决不得拷贝”）的受控内容。

如果存储的内容安全地绑定于执行记录的产品上，在它变得无法可用之前，无法移动并且自身无法在产品内做进一步的临时或其他记录，那么这样一个设备可以在内部存储此类内容，包括出于暂停程序运行的目的；前提是设备依据规定的稳健性要求进行制造，不会破坏此类限制。当在内部存储此类内容时，包括出于本节允许的暂停执行目的，内容应以如下方式进行加密和存储，即提供不小于 128 位的高级加密标准（AES）的安全性。

设计和制造的产品必须能删去所存储的内容，或在一段声明的时间周期后，基于逐帧、逐分钟、逐兆字节的方式，能使所存储的内容变得无法使用。

7.3.5 拷贝一次

7.3.5.1 拷贝功能

对在 EMI 位中已指定允许进行一次拷贝（“拷贝一次”）的内容，产品可以生成一份受控内容的拷贝，如第 7.3.2 节或第 7.3.4 节中所规定的那样，或假定拷贝：

a） 已经加扰、加密或惟一地绑定于该设备上，如果有的话，每种情况下均使用一种由第 7.3.5 节修正案确定的拷贝保护形式；以及

b） 如果有的话，通过一种由第 7.3.5 节修正案确定的方式，标出不得多次拷贝（“不得拷贝多次”），并将有效防止如下设备多次拷贝，即设备能够接收由第 7.2.4 节确定的输出口传输的此类标记数据。在没有此类第 7.3.5 节修正案的情况下，对第 7.3.2 节或第 7.3.4 节允许之外的其他受控内容，不得进行拷贝，除非第 7.3.5.2 节另有规定。

7.3.5.2 移动功能

只有在以下情况时，依据第 7.3.5 节对在 CCI 中标记了“拷贝一次”的内容进行一次拷贝的产品，才能将此类内容移至一个单个的可移动记录媒质中，或移至一个单个的外部记录设备中：

a） 外部记录设备表明它有权依据本节的要求执行该移动功能，并依据第 7.3.5 节的要求拷贝此类受控内容；

b） 为传送产品的传输，此类受控内容标明了“拷贝一次”；

c） 依据第 7.2.2 节、第 7.2.3 节或第 7.2.4 节，受控内容通过得到了保护的输出口输出；

d） 在移动完成之前，始发产品记录被致使无法使用，并且移动的受控内容标记为“不得拷贝多次”；

e） 移动记录媒介的移动目的设备不能或被致使不能输出受控内容，除非通过依据这些依从规则授权的输出口；以及

f） 拷贝用以下方式进行存储：

i） 使用这些依从规则修正案批准的加密协议，它惟一地将此类拷贝与单个设备相关联，因此它不能在另一个设备上播放，或如果存储于移动媒介上，那么不得制作更多的可用拷贝；或者

ii） 否则使用第 7.3.5.1 节中引用的方法。

当前的实施方案限制了对单个移动的移动数量。用于内容控制的其他方法正在研究中，在确定了下一代 DRM 系统后，它们即可应用。

8 变更控制

应使用此处所述的准则和过程对技术上的任何重大或实质性改变进行重新评估。重大或实质性改变包括但不限于：

1） 映射至一个新的传送网络或媒介；

2） 内容编码或处理上的改变；

3） 对技术的完整性或安全性有重大和负面影响的改变；

4） 所用密码方法上的改变（算法未变而只有密钥长度变长了的改变除外）；

5） 重新分配的范围发生了改变；以及

6） 技术特性上的任何根本性改变。

附 件 A

拷贝控制信息

拷贝控制信息（CCI）由视频服务提供商通过数据信道传送，告知机顶盒要求的拷贝保护等级。CCI 畅通无阻地传送给机顶盒，但通过利用一个简单的协议对 CCI 进行认证来维护信息的完整性。对每个来自机顶盒的元素下行流均重复此过程。

机顶盒和下行流元素利用 1 字节长的 CCI 字段所包含的信息来控制对内容的拷贝。2 个 EMI 位用于控制机顶盒数字输出的拷贝，2 个 APS 位用于控制模拟输出的拷贝，1 位作为受限的图像触发器，3 位保留。

A.1 信道变更

当信道发生变化时，机顶盒将对所有的 CP 散列内容进行处理，就好像 EMI 被设为“决不能拷贝”一样，但在接收到新的 CCI 消息之前不得应用图像限制。一旦自视频服务提供商处接收到 CCI 值，机顶盒将立即开始使用它。如果在 10 秒钟内未接收到新的 CCI 消息，那么机顶盒必须应用图像限制，就好像 CIT 位被设为 1 一样。信道变化不得引起密钥更新。

A.2 CCI 定义

CCI 是一个单个字节，8 位，是从机顶盒传送给下行流网络元素的字段。对 8 位中的 5 位进行了定义。剩余的 3 位保留。保留的 3 位设为 0，如表 A.1 所示。只有在执行如下所述的认证隧道协议时，下行流元素才使用接收自视频机顶盒的保留位值。之后，机顶盒必须忽略保留位值。

表 A.1/J.197－CCI 比特分配

CCI 位 #	7	6	5	4	3	2	1	0
VSP 设置为	0	0	0	CIT	APS1	APS0	EMI1	EMI0
STB 解释为	rsvd	rsvd	rsvd	CIT	APS1	APS0	EMI1	EMI0

A.3 EMI — 数字拷贝控制位

CCI 字节的 2 个 LSB 是 EMI 位。它们用于控制是否允许拷贝数字拷贝。EMI 位将提供给任何机顶盒数字输出口，用于控制自这些输出生成的拷贝。EMI 位在表 A.2 中定义。

表 A.2/J.197－EMI 值和内容

EMI 值	数字拷贝允许	内 容 类 型
00	拷贝不受限	非“高价值”
01	不允许进行任何更多的拷贝	高价值
10	允许进行一次拷贝	高价值
11	禁止拷贝	高价值

A.4 APS — 模拟保护系统

表 A.1 所示的 CCI 第 3 位和第 2 位分别是 APS 第 1 位和第 0 位。机顶盒必须使用 APS 位来控制模拟复合输出的拷贝保护编码，如表 A.3 所述。

表 A.3/J.197－APS 值定义

APS	描　　述
00	拷贝保护编码关闭
01	AGC 处理开启，分离关闭
10	AGC 处理开启，2 线分离关闭
11	AGC 处理开启，4 线分离关闭

A.5 CIT — 受限的图像触发器

表 A.1 所示的 CCI 第 4 位是 CIT 位。机顶盒必须使用 CIT 位来控制高清晰度模拟部件输出的图像约束。

表 A.4/J.197－CIT 值和应用

CIT 值	图像限制应用
0	没有宣称任何图像限制
1	要求图像限制

A.6 经验证的隧道协议

机顶盒利用接收的 CCI 值计算 CCI 认证值，并将之与接收自视频服务提供商的 CCI 认证值进行比较。若两个值不相同，则产生一个错误条件，机顶盒将 EMI 设为 11，如果值等于 1，那么启用图像限制。

附 件 B

稳健性检查清单

在发布任何产品之前，技术实现者都必须进行测试和分析，以确保实现的稳健性。下面的稳健性检查清单可以在执行测试中为实现者提供辅助，它覆盖了稳健性的某些重要方面。由于稳健性检查清单并不能解决相应产品制造商要求的所有要素，因此极力建议实现者对其测试程序及其产品的依从性进行彻底的评估。

一般实施问题

1） 设计和制造的产品是否没有开关、按钮、跳线、或相当于前述内容的软件、或可以切断的痕迹，利用这些可以破坏内容保护技术、模拟保护系统、输出限制、记录限制或依从规则的其他强制性规定，或者利用这些可以将受控内容透露给未经授权的拷贝?

2） 设计和制造的产品是否没有服务菜单和功能（如遥控功能、开关、检查盒或其他方式），利用这些菜单和功能可以截获受控内容流，或将其透露给未经授权的拷贝?

3） 设计和制造的产品是否没有服务菜单和功能（如遥控功能、开关、检查盒或其他方式），利用这些菜单和功能可以关闭任何模拟保护系统、输出限制、记录限制或依从规则的其他强制性规定？

4） 产品是否有可以改变或透露设备中受控内容流的服务菜单、服务功能或服务工具？

如果有，那么请描述这些服务菜单、服务功能或服务工具以及为确保这些服务工具不会被用来透露或误导受控内容而采取的措施。

5） 产品是否有可以关闭任何模拟保护系统、输出限制、记录限制或依从规则的其他强制性规定的服务菜单、服务功能或服务工具？

如果有，那么请描述这些服务菜单、服务功能或服务工具以及为确保这些服务工具不会被用来破坏产品加密特性（包括对依从规则的依从性）而采取的措施。

6） 产品是否有任何用户可及的总线（如稳健性规则第 6.2 节中所定义的）？

如果有，那么在该总线上是否承载受控内容？

如果承载，那么：

确定并描述总线以及受控内容是压缩的还是非压缩的。如果数据是压缩的，那么详细解释如何以及通过什么方式、按照稳健性规则第 6.2 节的要求对数据进行再加密。

7） 详细解释产品如何保护所有密钥的机密性。

8） 详细解释产品如何保护产品中所用的、机密的密码算法的机密性。

9） 如果产品将受控内容从产品的一部分传送给另一部分，不论是在软件模块之间、集成电路之间还是其他部分之间，或其组合之间，那么解释产品的各部分是如何执行认证和解密的，以及 MPEG（或类似的）解码器是如何设计的、相互之间是如何关联和集成的，以便按照稳健性规则第 6.3.1 节的要求保证受控内容的安全，使之免受截获和拷贝。

10） 是否有内容保护功能是以硬件形式实现的？

如果是，那么完成有关硬件实现的问题。

11） 是否有内容保护功能是以软件形式实现的？

如果是，那么完成有关软件实现的问题。

软件实现问题

12） 在产品中，描述以受保护方式存储所有密钥的方法。

13） 使用 grep 工具（UNIX 的一个工具程序）或相当工具，你是否无法发现任何永久性存储设备的二进制图像中的任何密钥？

14） 在产品中，描述以软件形式实现的、用于弄乱机密的密码算法和密钥的方法。

15） 在产品中，描述以受保护方式创建和维持中间密码值（如在产品模块或设备间认证过程中创建的值）的方法。

16） 描述用于防止通常可获得的调试或反编译工具（如 Softice）的方法，防止用这些工具来单步执行、反编译或检查以软件形式实现的内容保护功能的运转情况。

17） 描述产品用于自检组成部件完整性的方法，通过这种方式，更改将产生有关认证或解密的故障信息，如稳健性规则第 6.3.2b 节所述。描述当完整性遭到侵犯时将发生什么。

18） 确保执行完整性自检，执行测试，确保一旦某个二进制编辑器用于修改包含内容保护功能的可执行图像中的随机字节，那么可执行图像将无法工作，并描述测试的方法和结果。

硬件实现问题

19） 在产品中，描述以受保护方式存储所有密钥的方法，以及如何维护其机密性。

20） 使用 grep 工具（UNIX 的一个工具程序）或相当工具，你是否无法发现任何永久性存储设备的二进制图像中的任何密钥？

21） 在产品中，描述以集成电路或固件的形式实现所用的机密的密码算法和密钥，使之无法读取。

22） 在产品中，描述以受保护方式创建和维持中间密码值（如在产品模块或设备间认证过程中创建的值）的方法。

23） 描述用于防止替换、移去或改变硬件元素或模块企图的方法，这些硬件元素或模块用于实现内容保护功能。

24） 在产品中，硬件元素或模块的移去或替换是否将危及产品的内容保护特性（包括依从规则和稳健性规则），对产品造成损害，因此使产品无法接收、解密或解码受控内容？

附 录 I

数字输出

有必要对数字输出进行测试，看其是否与本建议书确立的要求相一致。已对下列数字输出清单进行了测试，看其是否与本建议书相一致，并提供了相应信息。今后，额外的输出也有望与本建议书的要求相一致。

I.1 有线电视实验室已对下列输出进行了测试，发现它与本建议书相一致：

- **带 DTCP 的 1394：**产品可以输出受控内容，并可以以数字形式通过 IEEE 1394 接口将受控内容传送给某个输出口，其中的输出受 DTCP 保护。产品务必支持 DTCP “完全认证”，并可以额外地支持 DTCP “受限认证”。若 DTCP 适当的许可证要求的话，不受控内容必须不带 DTCP 保护地输出给 IEEE 1394 输出口。

I.2 有线电视实验室已对下列输出进行了测试，发现它与本建议书相一致：

- **带 HDCP 的 DVI/HDMI：**产品可以输出经服务接收的内容，并可以以数字形式通过 DVI（包括 HDMI 接口）将经服务接收的内容传送给某个输出口，其中的输出总处于 HDCP 激活状态并开启。产品务必将所有合法接收的 HDCP SRM 传送给 HDCP 功能。

附 录 II

评估准则

依据所提交的特定输出或技术，评估准则应包括如下内容：

II.1 视频传送

定义的方法是否用于转换来自机顶盒的 CCI 并将其传送给提议的设备环境或概要？

i） 压缩的数字输出

- 是在接口处使用最初的数字压缩系统，还是重新压缩信号？
- 如果重新压缩，那么需要怎样的系统、概要、分辨率和数据率？
- 如果保留最初的压缩，那么是通过接口进行完全的多路传送，还是在多路合并后将接口限制于单个程序流？
- 如果输出承载全部的传输流，那么系统信息（如 OOB 数据）如何传输？
- 用什么方法来确保不中断该接口上的程序流，而不管在该接口上是否会出现其他的通信流量（QoS）？
- 接口处提供的最低保证数据吞吐量是多少？
- 用什么方法来实现对模拟和数字封闭标题数据、内容建议速率、带内紧急警报系统消息的传送、解密或显示？
- 如何无缝地在该接口上保留模拟编程服务？

ii） 不压缩的数字输出

- 接口处提供的最低保证数据吞吐量是多少？
- 如何无缝地在该接口上保留模拟编程服务？
- 用什么方法来实现对模拟和数字封闭标题数据、内容建议速率、带内紧急警报系统消息的传送、解密或显示？

II.2 安全接口

- 如何在视频传送中使用安全性？传送如何与内容保护概要以及内容保护概要的认证和保护方法相关联？
- 用什么方法来生成密钥、保护密钥和交换密钥？
- 是否存在明显的、内容是清晰的地方？

II.3 攻击点和系统弱点

- 技术是否能在某些地方被欺骗？
- 可能被攻击的最薄弱环节在什么地方？
- 黑客将攻击什么地方？需要什么资源？
- 可能的弱点/威胁是什么？如何权衡安全性与应用成本？

II.4 所提议技术的有效性

- 提议的技术能否适当地保护通过数字输出口传送的内容，或者安全地予以记录或存储，以供之后重放？
- 内容重新分配的范围是什么？数字输出或 DRM 技术能否通过局限控制或者其他地理性的或用户性的限制，来有效保护内容免受未经授权的重新分配？

II.5 安全性处理

- 在密码计算期间，密钥和秘密是否得到了保护，使之免遭读写？
- CCI、图像限制和其他控制措施是否在整个系统设计中都得到了保护？

II.6 密钥的撤销和更新

- 产品是否提供了系统密钥撤销解决方案？
- 产品是否提供了系统密钥更新解决方案？
- 使用什么样的撤销和更新准则与过程？谁是过程的参与者？
- 系统更新消息（SRM）的最小和最大长度是多少？它以怎样的格式进行传送？
- SRM 通常如何进行传送？撤销/更新解决方案对视频服务提供商网络（包括可能需要的重要设备或网络升级）有哪些操作和基础设施方面的影响？为了采纳提议的撤销和更新解决方案，视频服务提供商务必做哪些工作？

II.7 新的算法

- 算法的相对强度是多大？
- 相对其他技术，认证的相对强度是多大？

II.8 保持业务完整性

- 提议的输出/技术是否有碍机顶盒满足其他许可证发放或测试义务要求？对提议的数字输出，是否需要模拟源交换或高清晰度穿过？
- 输出是否提供了一种用于保留服务提供商导航和服务应用的方法？
- 提议的输出/技术是否与其他商用设备和接口有冲突？
- 提议的输出/技术是否会引起与其他商用设备和接口之间的互操作性问题？
- 提议的接口是否能够与来自其他制造商的产品互操作？或者它是一个专用的或排他的解决方案？
- 互操作性是否由行业标准（哪几个？）或许可证或二者定义？
- 技术是否需要进行一致性或依从性测试，以便确保互操作性？

II.9 许可证发放条件

- 许可证发放条件应与国际电联惯例和国家要求相一致。

II.10 对视频分配网络总的影响

- 在操作和基础设施方面，提议的技术将对视频分配网络产生哪些影响（包括可能需要的资金投入或网络升级）？
- 为了采纳提议的技术解决方案，视频服务提供商务必做哪些工作？

附 录 III

技术评估提交的要素

本建议书的评估过程涵盖的技术包括受保护的数字接口、安全的记录、内容存储和重放、数字权利管理。这些技术所用的特定的安全措施可以各不相同。另外，不同的输出技术可以使用不同的传输机制和协议，它们需要某些限定或实施限制。本附录确定若干关键的要素，它们对所有正在研究的候选技术都是适用的，但它不是一个排他性的清单，它不排除其他类型的信息，为对某项特定技术进行彻底评估，可能需要用到这些信息。提交的内容绝不能省略或不叙述实质性的规范、事实或其他细节，为对技术进行彻底、准确的评估，这些内容都是必需的。

接受评估的技术可以溶入有关受保护数字接口、安全的记录和内容存储、数字权利管理技术的混合要素。下面各节描述了应提交的建议要素，以便对候选技术进行彻底的评估。

III.1 许可证发放条件

许可证发放条件应符合国际电联的惯例和国家要求。

有关稳健性和依从规则的注释 — 包含任何数字输出、DRM 或内容保护技术的机顶盒设备下行流也务必符合本建议书为机顶盒建立的稳健性和依从规则要求。为机顶盒建立的稳健性和依从规则用于控制总的下行流生态系统。结果是，任何制造商技术许可证中的稳健性和依从规则都绝不能与本建议书中所述的稳健性和依从规则相矛盾。

III.2 安全性概述

安全性规范和文件应包括一个引言和安全性概述，它包括以下内容：

1） 安全性体系结构概述、其组成部件（如封装服务器、许可证服务器、客户机等）、它们的功能、关键接口；有关输出/安全性的连接要求。

2） 安全性体系结构的详细方框图，用于确定关键的组成部件和接口，它们是实现端到端解决方案所必需的，包括接收机和其他媒介元素（PC、存储器、显示器等）。

3） 概述还应清楚地确定视频传送选项，实现中它们有多种可选方案。例如，视频传送密码算法（AES、3-DES 等）、密钥交换算法（Diffie-Hellman、RSA 等）。

4） 详细描述机顶盒内容保护规则或许可证与提议的、将嵌入到“下行流”设备中的、内容保护技术之间的映射关系，尤其需要解决有关维护总的安全性和整个分配生态系统的内容保护方面的问题。

III.3 视频传送

安全性规范应包括有关视频传送方法的细节以及有关如何将机顶盒传送的拷贝控制信息（CCI）转换至提议的环境/概要的细节。规范还应详述视频传送如何与任何内容保护概要以及内容保护概要的认证和保护方法相关联。

另外，还务必提供规范或其他技术描述，以便详细解释提议的数字输出如何支持一个或多个视频传送协议，这些协议能够传送与机顶盒关联的所有已定义[1]音频—视频服务，而无需中断、阻止或削弱向最终显示设备的服务传送。此类服务还包括但不限于模拟和数字封闭标题数据、内容建议速率、紧急警报系统消息的传送、解码或显示。

应对内容保护技术所含的每种传输机制和协议进行技术评估。此类评估应逐个传输地进行，或逐个媒介地进行。如果某项特定技术在此成功满足准则要求，该技术也应不被认为对任何传输或协议获得了“全面批准”。

III.4 内容保护概要

安全性规范应包括有关系统中所用的任何数字签名内容保护概要格式和使用的细节。安全性规范还应定义该系统所用的结构和选项，以及实现方案所需的所有消息和信令。

III.5 密钥交换算法

安全性规范应包括有关接收设备、存储设备以及与之相连的任何设备认证的细节。安全性规范还应包括许可证服务器、封装服务器和客户机的认证方法。交换的所有会话密钥和使用的密码协议应良好定义，以便彻底评估。也可以使用非加密选择方案，但应做彻底解释。

III.6 安全接口

规范应包括有关详细定义整个系统安全接口、创建和保护对称与非对称密钥的细节。需定义以硬件形式和软件形式实现的、安全部件的详细定义，以便对这些安全接口进行检查。

III.7 安全性处理

规范应包括有关证明密钥和秘密在密码计算期间如何得到保护、使之免遭读写的细节，以及有关CCI、图像限制和其他参数在整个系统中如何得到保护的细节。

III.8 证书管理

规范应包括有关详细定义证书用法、专用密钥保护方法、撤销方法以及证书如何与内容和封装/证书服务器相关的细节。还应包括有关安装、签署、链接至根以及总体结构、安全性确认、如何防止证书被克隆的细节。

---

[1] 参见例子，ANSI/SCTE40-2004；第8.1节。

III.9 密钥的撤销/更新

规范应详细规定如何实现密钥撤销以及如何实现密钥更新。

III.10 攻击点/潜在的弱点

规范应包括评估或威胁分析，这些对评估可能的弱点/威胁和权衡应用成本是有用的。还应提供独立的安全评估。必要的话，评估中应做出不透露限制。

III.11 商业用途

提交的内容应包括有关提议的输出或技术的、任何已知的商业用途，以及任何已知的、对设备性能和互操作性的影响。提交方应提供采纳方（实施方）和支持方（所有者、内容开发商等）的清单，并确定技术提交方与任何内容所有者之间的任何商业关系。

III.12 联络信息

提交的内容应包括安全专家以及其他与提交事宜有关的个人的姓名和联络信息。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	**有线网和电视、声音节目及其他多媒体信号的传输**
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦