国 际 电 信 联 盟

ITU-T X.1191

国际电信联盟
电信标准化部门

(02/2009)

X系列：数据网、开放系统通信和安全性

安全应用和服务 – IPTV安全

IPTV安全方面的功能性要求和架构

ITU-T X.1191建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI 组网和系统概貌	X.600–X.699
OSI 管理	X.700–X.799
安全	X.800–X.849
OSI 应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	**X.1180–X.1199**
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339

欲了解更详细信息，请查阅 *ITU-T*建议书目录。

ITU-T X.1191建议书

IPTV安全方面的功能性要求和架构

摘要

ITU-T X.1191建议书研究涉及IPTV内容、服务、网络、终端设备和订户（最终用户）的安全方面的功能性要求、架构和机制。

来源

ITU-T 第17 研究组（2009-2012年）按照世界电信标准化全会（WTSA）第1号决议规定的程序，于2009年2月20日批准了ITU-T X.1191建议书。

关键词

认证、授权、加密、IPTV、隐私保护、安全、安全架构、扰码、服务和内容保护。

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ITU-T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

本建议书为简明扼要起见而使用的“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”等其他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他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，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

IPTV服务、通过此类服务传递的内容、在处理和提供此类服务时所用的终端设备要求考虑许多安全问题。本建议书制定了要求、架构模型、功能实体、接口、机制，并起草了附加的背景参考资料，说明与探讨这些安全方面的问题。

ITU-T X.1191建议书

IPTV安全方面的功能性要求和架构

1 范围

本建议书探讨涉及IPTV内容、服务、网络、终端设备和订户的安全与保护方面的功能性要求、架构和机制。可以预料，本建议书确定的要求和相关功能能够按照需要不同级别安全能力的IPTV服务和经营模型适当地实施。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，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均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某一自成一体的文件并非赋予该文件建议书的地位。

[ITU-T X.509] ITU-T X.509建议书（2008年）/ ISO/IEC 9594-8:2008，《信息技术 - 开放系统互连 - 号码簿：公开密钥与属性证书框架》。

[ITU-T Y.1910] ITU-T Y.1910建议书（2008年），《IPTV功能架构》（IPTV functional architecture）。

3 术语和定义

3.1 其他资料规定的术语

本建议书采用其他资料规定的下列术语：

3.1.1 access control 访问控制 [b-ITU-T X.800]：阻止未经核准而使用某个资源，包括阻止以未经核准的方式使用某个资源。

3.1.2 application 应用 [b-ITU-T Y.101]：一个结构化的能力集，可提供得到一种或多种服务支持的增值功能性。

3.1.3 authentication 认证 [b-ITU-T X.800]：见“数据源认证”和“对等实体认证”。

3.1.4 authorization 授权 [b-ITU-T X.800]：权利的授予，包括根据访问权准予访问。

3.1.5 availaibility 可获取性 [b-ITU-T X.800]：授权实体按照需要可访问或可使用的属性。

3.1.6 confidentiality 机密性 [b-ITU-T X.800]：不向未经授权的个人、实体或过程提供或披露信息的属性。

3.1.7 data origin authentication 数据源认证 [b-ITU-T X.800]：确认收到的数据源与自称的一致。

3.1.8 denial of service (DoS) 拒绝服务 (DoS) [b-ITU-T X.800]：阻止经授权的资源访问或拖延时限操作。

3.1.9 digital signature 数字签名 [b-ITU-T X.800]：附加在数据单元上的数据或数据单元的一种密码转换（见“密码学”），使数据单元接收方能够证明数据单元的来源和完整性，并防止作伪，例如接收方作伪。

3.1.10 elementary stream 基本流 [b-ITU-T H.222.0]：用于已编码视频、已编码音频或PES包中其他已编码比特流之一的一个通用术语。

注 – PES表示分组基本流。

3.1.11 functional architecture 功能性架构 [b-ITU-T Y.2012]: 用于描述NGN结构的一组功能实体及功能实体之间参考点。这些功能实体由参考点隔开，并由此规定了功能的分布。

3.1.12 functional entity 功能实体 [b-ITU-T Y.2012]：由一组不可分的特定功能组成的实体。功能实体是逻辑概念，而功能实体的分组则用于描述实际的物理实施方案。

3.1.13 integrity 完整性 [b-ITU-T X.800]：数据不曾以未经授权的方式被改变或销毁的属性。

3.1.14 key 密钥 [b-ITU-T X.800]：控制加密和解密操作的符号序列。

3.1.15 key management 密钥管理 [b-ITU-T X.800]：依照某种安全政策，生成、存储、分发、删除、存档和应用密钥。

3.1.16 masquerade 冒名顶替 [b-ITU-T X.800]：一个实体伪装成为另一个不同的实体。

3.1.17 network provider 网络提供商 [b-ITU-T Q.1290]：维护和运行IPTV功能性所需的网络组成部分的机构。

注1 – 网络提供商也可选择作为服务提供商。

注2 – 尽管服务提供商和网络提供商被认为是两个单独的实体，但也可以是同一组织实体。

3.1.18 peer-entity authentication 对等实体认证 [b-ITU-T X.800]：确认关联中的一个对等实体就是自称的那个实体。

3.1.19 privacy 保密；隐私 [b-ITU-T X.800]：一种个人权利，用于控制或影响与该个人有关的哪种信息可以被收集和存储以及该信息由谁和向谁披露。

3.1.20 repudiation 否认 [b-ITU-T X.800]：参与通信的一个实体否认曾参与过全部或部分通信过程。

3.1.21 security label 安全标签 [b-ITU-T X.800]：绑定在某种资源上的记号（可能是一个数据单元），它命名或指定了该资源的安全属性。

注 – 记号和/或绑定可以是明确的，也可以是隐含的。

3.1.22 security policy 安全政策 [b-ITU-T X.800]：为提供安全服务而制定的准则。

3.1.23 service provider 服务提供商 [b-ITU-T M.1400]：对按照某种资费或某个合同向客户或其他用户提供电信服务的提供商的一种统称。服务提供商可以非强制性地运营一个网络。一个服务提供商可以非强制性地成为另一个服务提供商的客户。

3.1.24 threat 威胁 [b-ITU-T X.800]：潜在的破坏安全的行为。

3.2 本建议书规定的术语

本建议书规定了下列术语：

3.2.1 acquisition 获取：最终用户得到内容的过程。

3.2.2 content export 内容输出：从IPTV终端向有权使用IPTV内容的用户所拥有的另一终端安全地输出该内容的过程。

3.2.3 content protection 内容保护：确保某一最终用户只能使用他/她按照权利持有人授予的权利所获取的内容；内容保护包括防止非法的复制和分发、侦听、改动、未经授权的使用等。

3.2.4 content tracing 内容跟踪：允许确认（任意）内容来源和/或责任方（如最终用户），以便在出现未经授权使用内容，如复制内容或重新分发的情况下促进后续调查的过程。

注 — 内容跟踪信息既可以作为元数据，也可以作为取证水印附加在内容上。

3.2.5 entitlements 权利资格：指包括有条件访问信息在内的授权级别，一个订户可以采用该级别从他/她的IPTV终端设备访问特定的IPTV服务。

3.2.6 IPTV Terminal Device (TD) protection IPTV终端设备 (TD) 保护：确保某一最终用户在行使获准使用某些内容的权利时及在用物理装置和电子装置保护未得到保护的终端设备的完整性和保护未得到保护的内容与关键安全参数（如已存储的密钥）的机密性的过程中，其接受某种服务时所用的终端设备能够可靠、安全地使用这些内容。

3.2.7 linear TV 单收电视：一种广播电视服务，类似于有线电视运营商、地面运营商和直接到户卫星运营商提供的传统形式的电视服务；此处指节目内容按照预定的播出安排发送，拟供最终用户实时消费。

3.2.8 metadata for watermarking facilitation 水印辅助元数据：辅助下游设备随后嵌入水印而生成的元数据。

3.2.9 phishing 网页仿冒：冒名顶替一个值得信任的实体获取用户名、出生日期或信用卡详情之类的敏感信息或个人信息的行为。

3.2.10 rights 权利：指对某一内容项目完成一组预定的运用操作的能力；这些运用操作包括许可（如收看/收听、复制、更改、记录、摘录、抽样、保存一段时间、分发）、限制（如多次播放/收看/收听、数小时连续播放/收看/收听）和义务（如支付、内容跟踪），适用于内容并提供了最终用户获准得到的使用自由。

3.2.11 rights expression 权利表述：权利的具体、正式形式的句法体现。

3.2.12 SCP end-to-end 端对端SCP：“服务和内容保护”的操作模式，其中内容是由终端设备采用单一服务和内容保护系统按照获准的权利访问和交换的。

3.2.13 SCP bridging SCP桥接：“服务和内容保护”的操作模式，其中两个或更多服务和内容保护系统在单一的设备上运行，该设备成为这些服务和内容保护系统之间的桥梁；从一个服务和内容保护系统获取的内容可以按照获准的权利经由桥上的另一个服务和内容保护系统访问。

3.2.14 SCP interchange SCP互换：更为一般化的“服务和内容保护”操作模式，涉及两个或更多设备，每个设备上运行一个或多个服务和内容保护系统；一个设备通过其服务和内容保护系统获取的内容可以按照获准的权利通过另一个不同的服务和内容保护系统安全地传送给另一个设备或在另一个设备上访问。

3.2.15 scrambling 扰码：用于保护多媒体内容的过程；扰码通常采用加密技术来保护内容。

3.2.16 scrambling algorithm 加扰算法：扰码过程或解扰码过程所用的算法。

3.2.17 secure transcodable scheme 安全的可变码方案：一种在保持端对端安全的情况下不用解密即可让中间网络节点实现变码的安全方案；执行该方案时可以将可伸缩编码、渐进加密和分组过程组合到一起。安全的可变码方案既可以提供机密性，也可以提供消息完整性/认证。

3.2.18 service protection 服务保护：确保最终用户只能在他/她有权接收的范围内获取某种服务和其内驻留的内容；服务保护包括在IPTV内容穿越IPTV服务连接时避免未经授权的访问。

3.2.19 service and content protection 服务和内容保护：服务保护与内容保护的组合，或该组合的系统，或该组和的实施。

3.2.20 spoofing 欺骗：伪造（假冒）的源（如一个人或一个计算机程序）通过捏造数据成功地冒名顶替了一个合法的源所涉及的活动；这种欺骗是以获取信息和/或隐藏真正的源从而让伪造的源得以从事未经授权的活动为目的，如传播恶意软件（病毒）等。

3.2.21 tamper-resistant 防篡改：防止个人用户/攻击者实际/通过软件入侵篡改产品、包装或系统。

3.2.22 transcoding 变码：多媒体内容，如图片、文字、音频和视频，从原有格式转换为另一种不同的格式或质量的过程。

3.2.23 user privacy protection 用户隐私保护：确保最终用户所认为的私密（或机密）信息得到保密，同时又维持法律程序所要求的强制性披露。

3.2.24 video signature 视频签字：用于确认视频内容的元数据（或可视特性）；与通过改变原有视频内容而嵌入的水印不同，视频签字是从视频内容本身提取的，没有质量降低的风险。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

AAA 认证、授权和结算

AD 授权域

CBC 密码块链接

CDN 内容传递网

DNG 传递网网关

DNGF 传递网网关功能

DoS 拒绝服务

ECB 电子源码书

ECM 权利资格控制消息

EMM 权利资格管理消息

EPG 电子节目指南

HN	家庭网
HN-TD	家庭网络终端设备
ID	标识符
IPTV	网际协议电视
MIKEY	多媒体互联网密钥设置
NAT	网络地址转换
OFB	输出反馈
P2P	对等网络
PDA	个人数字助理
PIN	个人标识号
PKI	公开密钥基础设施
PVR	个人录像机
QoE	体验质量
QoS	服务质量
REL	权利表示语言
SCP	服务和内容保护
SCP-B	SCP桥接
SCP-EE	端对端SCP
SCP-IX	SCP互换
STS	安全的可变码方案
TD	合乎IPTV规范的终端设备
USB	通用串行总线
VoD	视频点播

5 惯例

在本建议书中：

关键用语“**要求**”**(is required to)** 表明是一项务必严格遵守的要求，若要宣布与本建议书一致，则不允许与该要求有任何偏离。

关键用语“**建议**”**(is recommended)** 表明是一项建议遵守的要求，但并非绝对必要。因此宣布一致性时可不提出该要求。

关键用语“**禁止**”**(is prohibited from)** 表明是一项务必严格遵守的要求，若要宣布与本建议书一致，则不允许与该要求有任何偏离。

关键用语“**可以非强制性地**”**(can optionally)** 表明是一项可允许的非强制性要求，没有任何建议遵守的意思。这种表述并非意味着供货商必须提供该选项，然后由网络运营商/服务提供商非强制性地启用该特性，而是意味着供货商可以非强制性地提供该特性，同时仍然宣布与规范一致。

在本建议书中的IPTV安全架构范围内：

规定“**功能**”为功能性的集合。由下列符号表示：

规定“**功能块**”为本建议书所述的详略范围内未做进一步划分的一组功能性。它由下列符号表示：

6 安全要求

6.1 总体安全要求

- 建议在IPTV架构中要考虑到对性能、服务质量、可用性、可调整性和实施安全措施的成本限制方面的影响/牵制。
- IPTV架构可以非强制性地支持最终用户共享内容的内容保护。

6.2 内容安全要求

本节具体规定分别涉及或共同涉及内容和内容保护的要求。

架构要求

- 要求IPTV架构支持第3节规定的内容保护。
- 要求IPTV架构支持内容与内容保护元数据和内容管理元数据之间的关联。
- 要求IPTV架构支持包括使用权元数据在内的内容保护元数据和内容管理元数据的安全传递。
- 要求IPTV架构支持对各种使用的权利加以区分的内容使用权元数据，这些使用包括给出（收看）、存储、（重新）分发及这几种方式的组合。
- 要求IPTV架构支持对同时分发给大量订户的内容的保护（可调整性）。
- 要求IPTV架构支持对多组播和/或单播流媒体内容的保护。
- 要求IPTV架构支持对按照获准的使用权存储的内容的安全保证。
- 若部署了内容跟踪，则要求IPTV架构以脱机（非实时）方式支持稳健的内容跟踪（例如 VoD内容）。
- 禁止IPTV架构妨碍对携载内容跟踪信息（例如水印辅助元数据）的手段的支持。
- 禁止IPTV架构妨碍对为了唯一地确定某一会话（例如信道、时间/日期）、终端设备

和/或网络运营商而在终端设备的输出级内采用内容跟踪技术的支持。这种内容跟踪技术的例子可能包括把可视和不可视信息作为一个选项。

- 禁止IPTV架构妨碍对内容中的所有内容跟踪信息的检索。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，在此情况下只允许授权用户或设备使用IPTV内容，即便内容转移到另一个安全系统也如此。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，以便让保留的标识信息可以始终如一地识别出IPTV内容，无论采用哪种标识方案，也无论内容被转移到了哪个安全系统。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，以便在内容被转移到另一个安全系统时避免安全级别降低。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，在此情况下只有可信设备被授予权利。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，以便为交换服务和内容保护互操作性数据（例如认证信息、元数据、密钥信息等）提供安全的环境。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，使互操作性不依赖于具体的软硬件。
- 禁止IPTV架构为了达到互操作性而要求两种互操作的SCP方案的任一端公开规定服务和内容保护机制。
- 禁止IPTV架构妨碍对可支持各种经营模型的灵活、可扩充服务和内容保护互操作性的支持。
- 禁止IPTV架构妨碍对采用不同安全机制的多种安全系统内的服务和内容保护互操作性的支持，目的是在即便采用不同的安全机制也支持无缝的随时播放服务（订户可以存储内容，供以后检索）和随地播放服务（订户可以在任何地点收看内容）。
- 禁止IPTV架构妨碍对服务和内容保护互操作性的支持，以维护对用户的透明度。
- 禁止IPTV架构妨碍对多种内容和服务保护机制的支持，无论具体的软硬件要求是什么。

架构建议

- 若IPTV内容采用了内容跟踪技术，则建议采用无法察觉的跟踪技术。
- 建议IPTV架构以实时的方式支持稳健的内容跟踪（例如广播内容）。
- 建议IPTV架构支持对内容共享服务（例如内容输出和内容重新分发）的最终用户的认证和授权能力，若支持内容共享的话。

- 若IPTV架构的实施方案采用基于水印辅助元数据的内容跟踪技术，则建议采用诸如具体的编码方案中提出的“用户数据”规定在内容基础流中嵌入相关的元数据。
- 如IPTV架构中一台TD或HN-TD支持多种内容和服务保护机制，建议使用一种标准化的转换功能，从而将一个以上的SCP系统连接起来，并进行统一转换，确保此转换机制中所连接的TD或HN-TD的互操作。

架构选项

- IPTV架构可以非强制性地支持纳入内容跟踪信息。这种内容跟踪信息可以非强制性地含有运营商ID、内容所有者ID、终端设备ID和其他信息。

加扰算法要求

- 要求广播流的加扰算法支持定期更新必要的密钥。
- 要求采用可公开获得的标准化密码算法构建IPTV的加扰算法。

加扰算法建议

- 建议IPTV的加扰算法具备足够大的密钥熵，以有效避免对内容进行密码分析。
- 不禁止IPTV架构妨碍对广泛使用的扰码算法的支持。
- 建议IPTV架构避免抑制对多种扰码系统的支持。
- 建议IPTV的加扰算法无论对于硬件实现还是软件实现都能有效实施。
- 建议IPTV的加扰算法，即密码参数（例如密钥长度、密码有效期等）或密码模式（例如CBC、OFB、ECB等），是可调整的和不会过时的。

加扰算法选项

- IPTV的加扰算法可以非强制性地对不同的内容类型采用不同长度的密码算法。

6.3 服务安全要求

本节具体规定分别涉及或共同涉及服务和服务保护的要求。

架构要求

- 要求IPTV架构支持第3节规定的服务保护。
- IPTV架构不得妨碍服务器端对TD中SCP升级或更新的支持。
- 要求IPTV架构支持最终用户（订户）授权和认证。
- 要求IPTV架构支持某种机制，可通知终端设备运用根据标准化的框架指定的加扰算法。

- 要求IPTV架构具备采用互操作性所需的标准密钥管理系统（如MIKEY、EMM/ECM）的能力。
- 要求IPTV架构支持在服务器侧通过SCP接口就IPTV的加扰算法和运营商选定的任何其他加扰算法对SCP系统进行更新和询问的能力。
- 要求IPTV架构支持与具体内容格式无关的SCP机制。
- 要求IPTV架构支持对敏感元数据提供完整性保护和数据来源认证的机制。
- 要求IPTV架构支持将权利信息和内容访问控制信息安全地传递给终端设备的机制。
- 要求IPTV架构支持内容使用控制（如重放）。
- 要求IPTV架构支持不同的重放模式，如限制播放次数、限制播放时间、限制快进和快退。
- 要求IPTV架构支持能维持SCP服务器与SCP客户机之间信令消息机密性的机制。
- 要求IPTV架构支持能维持SCP服务器与SCP客户机之间信令消息真实性的机制。
- 要求IPTV架构支持能维持SCP服务器与SCP客户机之间信令消息完整性的机制。
- 要求IPTV架构支持安全地检索终端设备SCP参数（如设备配置、状态）的机制。
- 要求IPTV架构支持安全地更新终端设备SCP参数（如设备配置）的机制。
- 禁止IPTV架构妨碍对以可编程方式（如根据时间、事件、内容或信道）打开或关闭内容跟踪功能的能力的支持。
- 若采用了密钥管理系统，则要求该系统具备可调整性、可靠性和互操作性。
- 禁止IPTV架构妨碍对不更换硬件而安装和运行多种服务保护解决方案的支持，可插拔设备（如USB狗和SIM卡）除外。
- 禁止IPTV架构妨碍对可用服务保护解决方案的识别机制的支持，这些解决方案能满足相关内容保护的规定要求。
- 禁止IPTV架构妨碍对SCP系统发现机制的支持，以便IPTV架构可以支持某种发现方法并在具体内容要求某种具体的服务保护系统时随时为适应该方法而做出调整。
- 禁止IPTV架构妨碍对不更换硬件即能从可用SCP系统中选定某个SCP系统的机制的支持，可插拔设备除外。
- 禁止IPTV架构妨碍对安全地下载SCP系统的支持。下载的SCP系统可以非强制性地取决于具体的服务保护要求。
- 若部署了可下载SCP，则要求IPTV架构对下载的SCP系统执行完整性保护和数据来源认证。

- 若支持终端设备安全地下载应用程序，则要求IPTV架构对下载的应用程序执行完整性保护和数据来源认证。

架构建议

- 建议IPTV架构启用内容机密性。
- 建议IPTV架构支持多种加扰算法。
- 建议IPTV架构支持对内容共享服务（例如内容输出和内容重新分发）的最终用户进行认证和授权的能力。
- 若IPTV架构采用了密钥管理系统，则建议考虑某种分级的密钥管理方案，以支持可调整性。
- 若IPTV架构采用了使用“组密钥管理协议”的密钥管理系统，则建议考虑某种分级的密钥管理和某种密钥管理算法替代方案，以支持可调整性。
- 若PTV架构采用了使用“短期密钥”的密钥管理系统，则建议提供媒体路径时NAT（网络地址解析）遍历和带宽的制约条件不对密钥交换构成限制。
- 建议IPTV架构（为了控制未经授权的访问）支持的对内容跟踪信息的保护程度至少与相应的被跟踪内容所用的保护相同。
- 建议IPTV架构支持同时传输内容和内容跟踪信息，在传送过程中保持内容与内容跟踪信息同步。
- 若IPTV架构采用PKI对终端设备或者对服务提供商或内容提供商进行认证，则建议采用多级结构的PKI，以支持可调整性、可靠性和互操作性。
- 若IPTV架构将PKI用于IPTV服务，则建议采用可公开获取的标准化证书格式、证书撤销清单或在线证书状态协议。
- 建议IPTV架构支持终端设备安全地下载应用程序。
- 建议IPTV架构支持将收看某些节目的权利限定在某些订户群体的机制（例如阻止某个特定地区的住户收看）。举例来说，该机制可以非强制性地用于体育赛事。

架构选项

- 为了向清晰度不同于用户终端的用户自有终端提供可调整的IPTV服务，IPTV架构可以非强制性地支持提供第3节规定的安全的可变码方案的能力。

6.4 网络安全要求

本节具体规定分别涉及或共同涉及网络或其保护的要求。

架构要求

- 要求IPTV架构支持减轻拒绝服务攻击的能力。
- 要求IPTV架构支持提供阻止非法或无用业务量的安全措施。

- 要求IPTV架构能够抵抗对组播能力的攻击。
- 建议多播架构支持在总体或重叠（对等实体之间的）多播环境中认证对等实体的能力。
- 若家庭网内终端设备之间的通信链路运载未受保护的加价内容，例如由消费者支付的内容，则要求保护该通信链路的内容安全。
- 要求IPTV架构支持IPTV管理功能对DNG的认证。
- 要求IPTV架构支持DNG对IPTV管理功能的认证。

架构建议

- 为了保护家庭网不受恶意或未经授权的访问，建议IPTV架构支持传递网网关功能（DNGF）能力，以建立可在远端配置、具有多级安全和适当的应用层网关的防火墙。
- 建议IPTV架构支持IPTV管理在远端配置NAT和远端配置DNG侵入保护功能的能力。
- 建议IPTV架构支持远端IPTV管理功能在远端配置NAT和DNG侵入保护功能的能力。
- 建议IPTV架构在支持远端管理的情况下确保终端设备远端管理的安全。
- 建议IPTV架构支持内容标签信息的使用，以控制内容的传递。

6.5 终端安全要求

本节具体规定分别涉及或共同涉及终端设备或其保护的要求。

架构要求

- 要求IPTV架构支持第3节规定的终端设备保护。
- 要求IPTV架构支持终端设备认证。
- 要求IPTV架构支持终端设备的物理改动抵抗力。
- 要求IPTV架构支持检测终端设备何时受到物理改动的手段。
- 若部署了可下载SCP，则要求IPTV架构支持终端设备安全地下载和安装SCP操作代码。
- 要求IPTV架构支持某种安全的手段来完成终端设备中与安全紧密相关的过程，如密钥管理和媒体序列化，以便在出现安全相关故障、检测到改动或出现其他滥用迹象时中止内容的播放。
- 要求IPTV架构在未提供逻辑保护（如加密或序列化水印）的情况下对终端设备中敏感的安全衍生过程和涉及重要内容的处理、传输及存储的部件提供物理保护。这些过程包括解扰码和媒体序列化。
- 要求IPTV架构认可对包括解扰码和媒体序列化（内容跟踪）在内的终端设备中敏感的安全衍生过程提供物理保护（以防止对终端设备的SCP功能系统的刺探和改动）的

必要性，认可对支持这些过程的关键数据和对涉及缺少逻辑保护（如加密或内容跟踪水印）的任何重要内容的处理、传输及存储的所有部件提供物理保护的必要性。

- 禁止IPTV架构妨碍对终端设备与其他（物理或逻辑）设备之间内容互换的支持，条件是该内容获准的用途中包括这种互换。
- 要求IPTV架构支持某种允许终端设备对SCP服务器进行认证的机制。
- IPTV架构不得妨碍对终端设备中SCP的更新的支持。
- IPTV架构必须支持数字或模拟输出，如数字或模拟视/音频输出传送至终端设备，SCP客户端外置存储设备要求对其进行保护。

架构建议

- 建议IPTV架构在终端设备中提供内容输出功能，以便让IPTV内容能够安全地从IPTV终端转移到有权使用该内容的用户所拥有的其他终端。

6.6 订户安全要求

本节具体规定分别涉及或共同涉及订户和最终用户或其保护的要求。

架构要求

- 要求IPTV架构支持第3节规定的用户隐私保护。
- 要求IPTV架构允许订户设置某种访问控制机制（例如使用口令），以限制对内容和/或服务的访问。
- 要求IPTV架构能够表明为什么拒绝用户访问内容。
- 要求IPTV架构支持某种能让订户请求扩展与特定内容实例有关的使用权（例如增加播放次数、增加播放时间）的机制。

架构建议

- 建议IPTV架构允许最终用户（在权力允许的范围内）变更，也就是替换终端设备，同时对消费内容的权力不构成本质影响。
- 建议IPTV架构支持某种按照内容对节目进行分级的机制。

注 — 分级信息可用于访问控制，例如家长管理。

7 安全架构

本节按照总体安全架构、内容保护架构和服务保护架构对IPTV安全架构做了规定，还规定了满足前几节所述要求的安全功能实体。

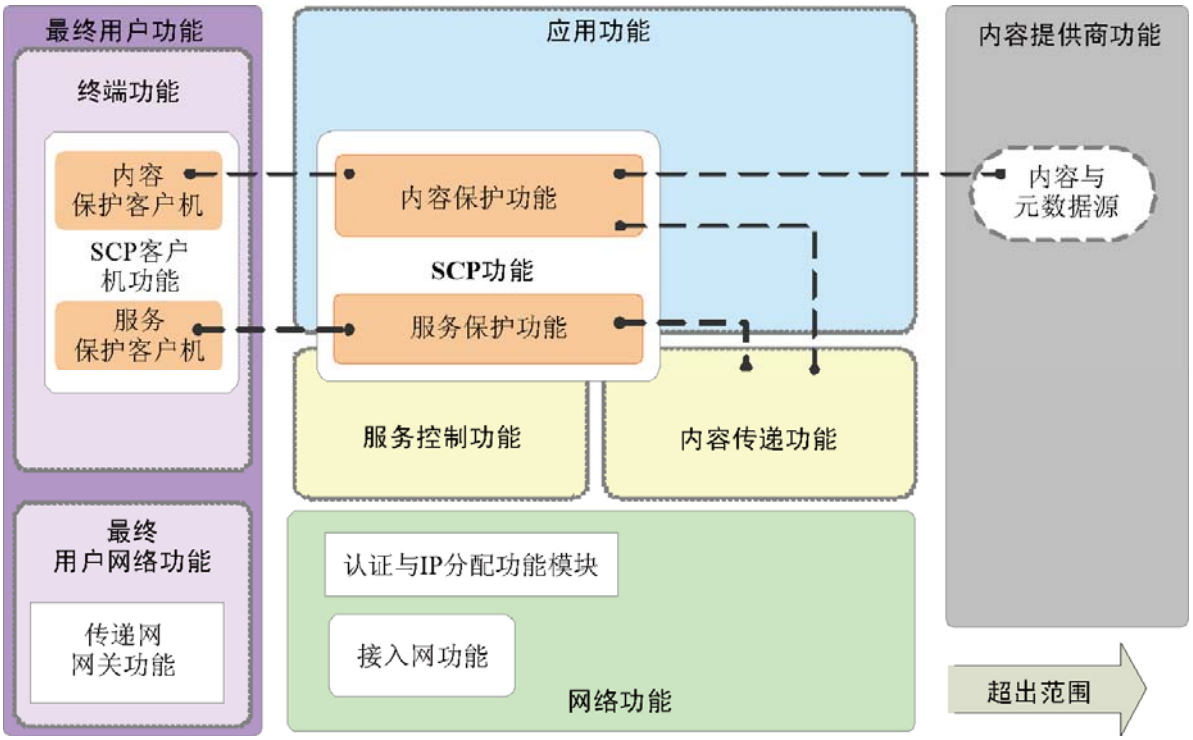
假定下文所述的IPTV安全架构用于[ITU-T Y.1910]第6节和第8节分别规定的IPTV功能域和IPTV功能性架构框架的范围内。

7.1 总体安全架构

下面的图7-1描绘了IPTV的一种总体安全架构。该总体架构分为两大区域 – 一个被认为就本建议书的用途而言在范围之内，另一个则被认为超出了范围。第一个区域包括最终用户域、网络提供商域和服务提供商域，而第二个区域则涵盖内容提供商域。

在第二个区域中，内容提供商域内和内容提供商与服务提供商互连中的所有安全问题都需要在这些域内运作的各利益相关方达成专门协议。因此，这些安全问题被认为超出了本建议书的范围。

尽管内容提供商域和内容提供商域与服务提供商域的互联在目前的环境下被认为超出了范围，但为了完整起见，下文各图和叙述中还是纳入了内容提供商域。这样，文中关于这些域的任何说法都要求看做资料性的或解释性的。



注1 – 本图中的内容保护功能和和服务保护功能是IPTV安全架构最重要的部分。关于这些功能的详细讨论可查看图7-2（内容保护架构）和图7-3（服务保护架构）。

注2 – 为了简化起见，本图省略了IPTV架构中某些与IPTV安全无直接关系的功能和功能模块。

图 7-1 – IPTV 总体安全架构

总体安全架构大致分为如下四个功能区域：

- 内容提供商功能（技术上超出了范围）

  假定内容提供商向与自己建立了关系的服务提供商提供对内容的访问。在某些情况下，内容提供商本身也作为服务提供商；此时，这种关系被认为是内部关系。

在向服务提供商提供对内容的访问时，内容提供商可采用标准机制或专门机制来控制和启动对内容的访问，不过要注意，这种机制被认为超出了本文件的范围，完全属于相关利益方之间的专门协议。

- 服务和内容保护（SCP）功能（与应用功能、服务控制功能和内容分发功能的某些部分重叠）

  SCP功能在IPTV总体安全架构，特别是在服务提供商域中起着核心作用。具体地说，服务保护功能启动对服务基础设施的保护和对服务和其内驻留的内容的访问控制。另一方面，内容保护功能按照许可的用途启动对服务和内容的使用控制。SCP功能中的这些具体功能和功能模块分成三个子区域：应用功能、服务控制功能和内容传递功能。

  服务提供商的义务是根据内容提供商的执照只在一定的使用条件下提供内容，如收看一次但不许录制、录制一次收看多次、录制一次后转让录制权等。SCP功能中内容保护方面的首要目的是让服务提供商以能够得到客观评价的方式完成这些义务。

  SCP功能中服务保护方面的首要目的是防止未经授权访问被下面各域中的实体认为是机密的服务资源和信息：服务、网络、终端设备和最终用户（订户）。

  SCP功能中服务保护方面的次要目的是避免服务基础设施受到有意和/或无意的资源滥用的损害。

  图7-2 （内容保护架构）和图7-3（服务保护架构）分别描绘了内容保护功能和服务保护功能的详细功能模块。

- 网络功能

  涉及网络域的安全功能的重点是对实体进行认证和对传递或将要传递IPTV服务的网络进行访问授权。次要功能是保护网络本身的完整性 – 采用物理装置、电子装置和运行手段（例如通过检测和挫败对接入网和承载网的拒绝服务攻击）完成保护。

- 最终用户功能

  应用于最终用户（订户）的安全方面包括保护在订户住所工作的终端设备的完整性及保护最终用户的隐私。

  在某些情况下，终端设备与网络域之间的DNG可被认为位于最终用户域内，受到最终用户安全措施的制约。

  最后，建议应用完整性机制来保证终端设备收到并随后重新分发给家庭网之内或之外其他设备的内容的完整性。（由此形成最终用户安全方面与内容安全方面的重叠。）

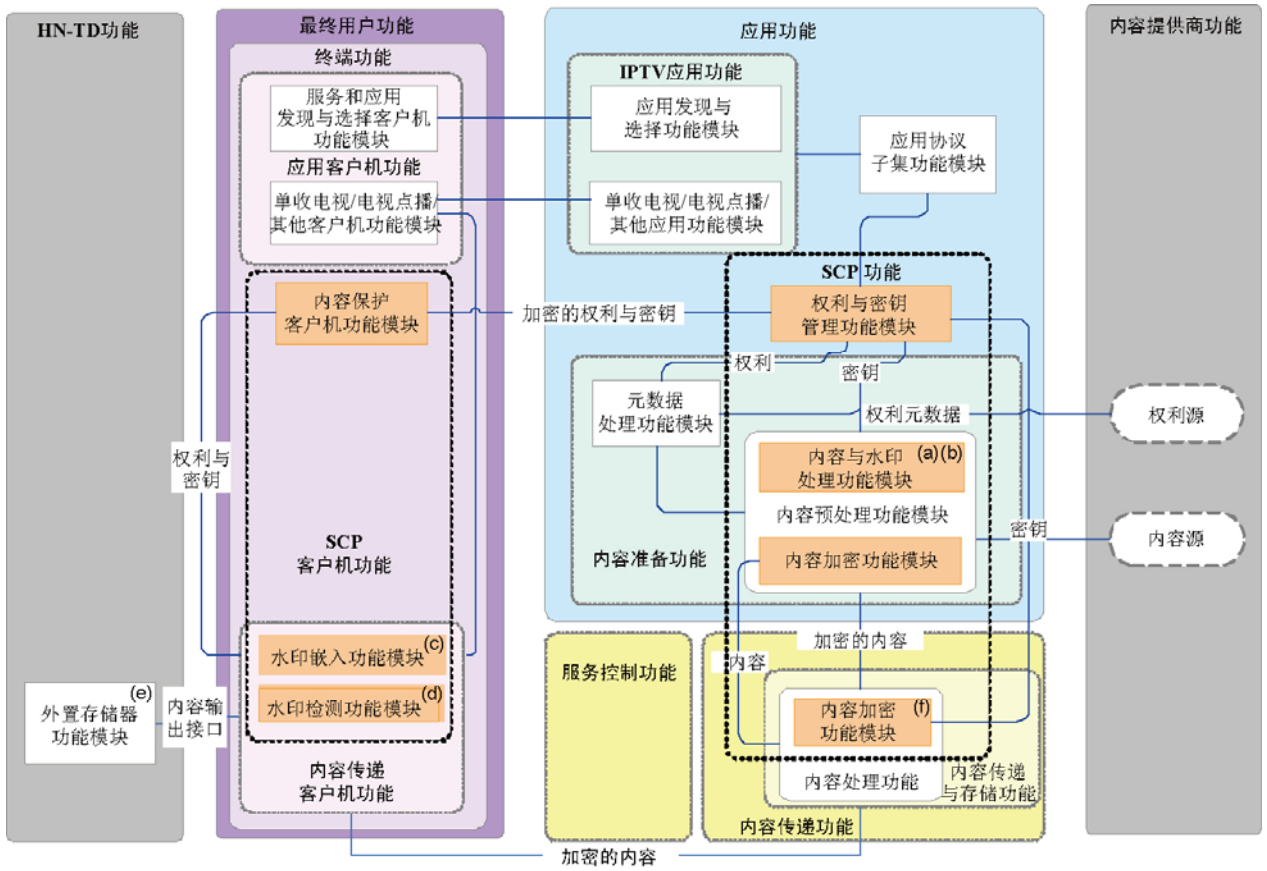
第7.4.1节更为详细地说明了图7-1所示的功能和功能模块。

7.2 内容保护架构

下面的图7-2描绘了IPTV的一种内容保护架构。

内容保护架构的首要功能是勾勒内容使用权所涉及的信息的流程和处理以及勾勒管理与促进这种权力所需的信息的流程和处理。

归根结底，内容使用的权利来自内容提供商；不过要注意，服务提供商可以根据与内容提供商达成的协议和经营策略更改（例如限制甚至扩充）这种权利。



(a) 非强制性水印元数据生成，便于下游嵌入水印
(b) 非强制性水印嵌入器，用于区分到网络服务器的内容和单播内容
(c) 非强制性水印嵌入器，用于区分多播内容实例
(d) 非强制性水印嵌入器，用于复制保护水印
(e) 非强制性外置存储器：HN-TD内的存储设备
(f) 位于内容传递与存储功能内的内容加密功能模块是非强制性的
注 — 灰色对象超出了IPTV安全架构的范围。

注 — 本图中的内容保护功能块由内容保护功能和内容保护客户机功能组成。

图 7-2 - IPTV 内容保护架构

上面示出的内容保护架构由主要驻留在两个功能区域内的功能组成：

- 服务和内容保护功能（与应用功能和内容传递功能重叠）

  内容及其相关权利是从内容提供商处收集的，经汇总和处理后传递给最终用户，其中总体过程由若干功能（如内容准备功能）采用说明最终用户权利和相关条件的数据进行管理。

  内容、权利和密钥（用于准予访问内容和启动内容的使用）信息被组织成适于特定应用的形式，例如收看单收电视。根据权利与密钥管理功能模块的授权（例如EMM）将权利和密钥信息传递给内容保护客户机功能模块；作为一个选项，对内容进行处理以插入内容跟踪（例如水印）元数据；然后在传递之前由内容准备功能对内容进行加密。在某些情况下（例如实时IP服务），作为一个选项，内容也可以由内容传递功能加密。

  在IPTV内容保护架构（不同于下文描述的IPTV服务保护架构）的范围内，重点主要集中在权利及密钥的管理、处理和传递上，而不是对该信息或对需要遵守这些权利的内容进行加密。

- 最终用户功能

  最终用户域内运行的终端功能负责实施与权利信息有关的内容使用规则（也称为内容保护元数据）。由该功能实体解释从权利与密钥管理功能模块获得的内容权利和密钥，然后按照解释采取行动，以控制如何处理内容和如何通过集成的显示装置（例如显示器或发声系统）或通过与外部设备的物理互联披露给最终用户。

  在终端设备将受保护的内容传输给外部设备（例如显示输出）的情况下，内容权利可能会转换为其他形式；作为一个选项，可能会对这种用途的内容做进一步处理，以插入客户机端内容跟踪信息（例如水印），或者重新对内容加密，以完成下游访问控制。

第7.4节更为详细地说明了图7-2所示的架构块。

在图7-2中，内容输出接口是连接IPTV TD与HN TD的逻辑接口。HN-TD本身可能会消费内容，也可能将内容输出到其他HN-TD。内容传递客户机功能可能会调整相应的安全标签，以确保只有授权HN-TD系统可以消费和输出内容。

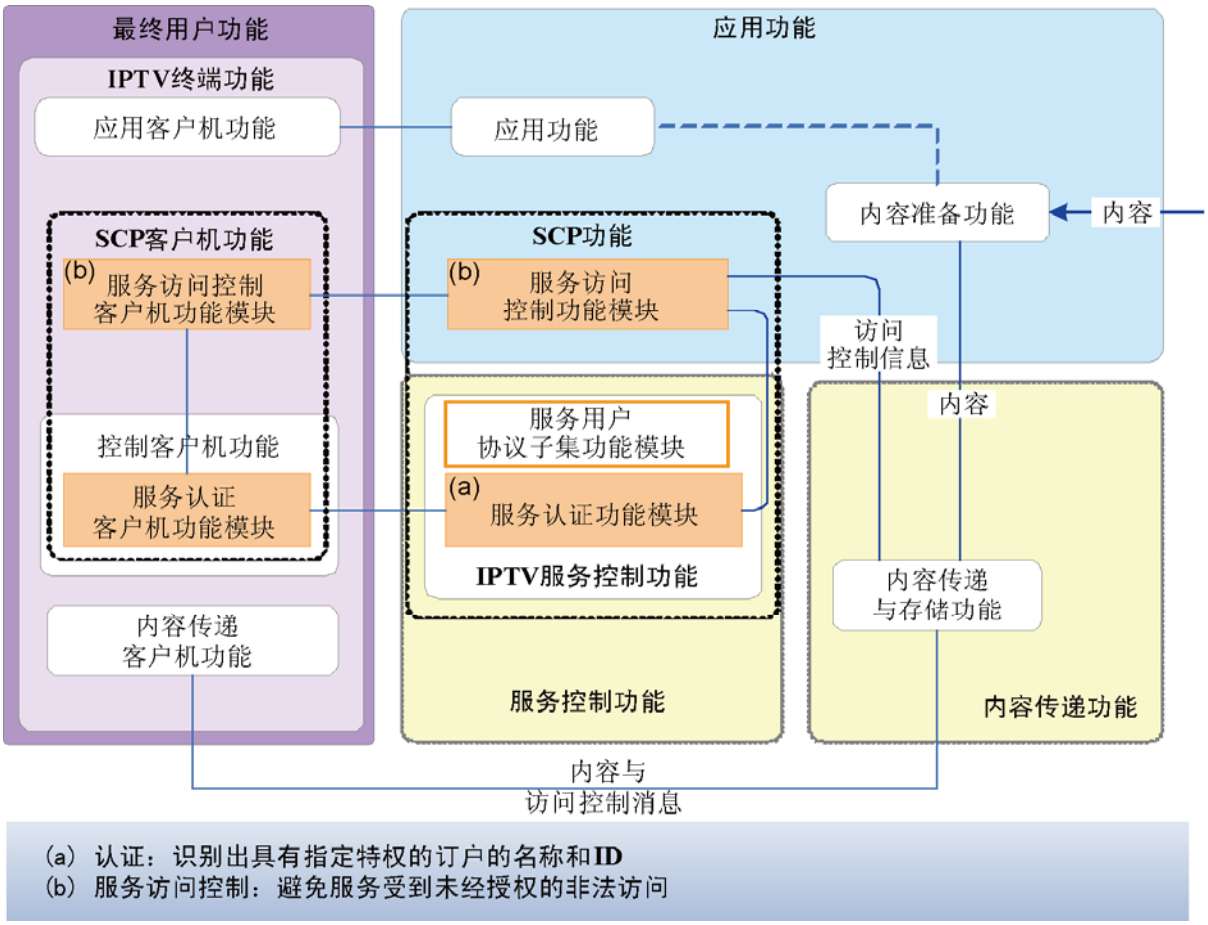
7.3 服务保护架构

对于涉及受保护内容的被管服务，一种典型情况是，在对服务和其内驻留的内容完成访问认证之后，必须对其中的最终用户（订户）和终端设备进行认证和授权。

可根据情况对终端设备和最终用户分别执行认证和授权操作。在其他情况下，对服务进行访问授权之前可能需要对最终用户住所的附加设备，如传递网网关和其他最终用户设备进行认证。

可以同时进行认证和授权，以控制为了在使用之前先获取服务和内容而对IPTV服务和终端设备二者的访问。

下面的图7-3描绘了IPTV的一种服务保护架构。



注 – 本图中的服务保护功能块由服务保护功能和服务保护客户机功能组成。

图7-3 - IPTV服务保护架构

服务保护架构的首要功能包括：

- 订户和终端设备认证

  该功能对订户和终端设备进行认证。

  - 订户认证：用户真实性验证过程
  - 终端设备认证：终端设备真实性验证过程

  在采用X.509基证书作为认证证书的情况下，撤销功能是必需的。

- 服务器认证
  - 在终端设备中，为了相互认证而对服务器进行认证的功能
- 服务访问控制
  - 授权用户通过扰码和加密之类的安全机制对获取服务和访问服务进行限制的功能

第7.4节更为详细地说明了图7-3所示的架构模块。

7.4 对IPTV安全架构中功能和功能块的说明

本节对上文第7.1节（总体安全架构）、第7.2节（内容保护架构）和第7.3节（服务保护架构）所述的架构模型中描绘的功能和功能块做更为详细的说明。这三节只对这些功能和功能块做了笼统的描述性规定，并划分成三部分，每节对应一部分。

7.4.1 总体架构功能和功能块

接入网功能：对由网络始发的控制与数据业务量进行收集和汇总；激活QoS/QoE，包括缓存管理、排队与时间安排、包过滤、业务量分类、做标记、监督和业务量成形。

注1 – 从IPTV服务和内容保护的角度看，这些功能与服务和内容保护功能无关。

应用功能：在服务器（服务提供商）端与客户机（最终用户住所）端之间划分；由准备、始发、接受和处理服务层IPTV应用（像单收TV、电视点播）及相关内容（例如可获得性信息、交互应用等）的功能部件组成。

认证与IP分配功能块：为连接到网络功能的传递网网关功能块提供认证功能性，并为IPTV终端功能分配IP地址。

内容保护功能：提供让内容使用政策得以实施的机制，这些政策包括权利与密钥的汇总、分发和管理，还可以非强制性地包括内容跟踪信息（例如水印）的生成与插入（嵌入）和（在服务保护功能控制之下的）内容加密。

注2 – 第7.2和第7.4.2节进一步讨论了构成内容保护功能的具体功能块。

内容保护客户机功能：与服务器端内容保护功能互动，以便实施内容使用政策。

内容提供商功能：向服务提供商传递内容和传递内容权利与密钥元数据。

传递网网关功能：提供终端设备与传递网之间的连接；管理本地（最终用户住所）的IP连接，获取终端设备的IP地址和IP配置。

注3 – 从IPTV服务和内容保护的角度看，该功能与服务和内容保护功能无关。

服务保护功能：为IPTV服务和其中所含的内容的认证与授权以及访问控制提供机制，包括管理和直接实施控制信号加密和内容互换加密，该功能要么与内容保护功能无关，要么与之配合。

注4 – 从IPTV服务和内容保护的角度看，这些功能与服务和内容保护功能无关。

注5 – 第7.3和第7.4.3节进一步讨论了构成服务保护功能的具体功能块。

服务保护客户机功能：与服务器端的服务保护功能互动，以完成服务访问控制和其他保护功能。

终端功能：提供服务保护和内容保护客户机，用于按照使用权元数据解密和实施服务与内容使用政策；按照需要完成链路层加密和SCP解析（互换），用于下一步的下游内容输出或重新分发和内部（或外部）内容存储，包括支持安全的（防改动的）媒体处理渠道、本地秘密（例如密钥）存储、安全软件更新能力、可下载软件资产的认证与验证、考虑到最终用户隐私的情况下对本地存储与互换的用户数据的保护。

7.4.2 内容保护架构功能和功能块

应用客户机功能：首要问题是协调和控制最终用户与IPTV应用功能所提供的服务之间的互动；对于标准的应用，如单收电视的收看，提供基本用户接口和最终用户获得服务所用的运行模式。

- **应用发现与选择客户机功能块**：允许最终用户和/或终端设备发现服务提供商提供的应用和应用服务是否存在并加以选择。

IPTV应用功能：嵌入了某些IPTV服务（例如单收电视、电视点播等）的始发点的逻辑实体；负责协调所有服务提供商的设施，以便有效地提供某些服务。

- **应用发现与选择功能块**：与上述应用发现与选择客户机功能块互动，以便让最终用户和/或终端设备能够发现应用和应用服务是否存在并加以选择。

应用协议子集功能块：存储和管理关于应用和服务的具有全局性质或针对特定最终用户（订户）的设备配置信息；通常用于允许应用服务器为最终用户定制服务和内容，常常会与各种账务系统互动或（内部）实现各种账务系统。

内容准备功能：在内容传递之前完成各种类型的内容预处理，诸如内容跟踪（例如水印）分析与元数据生成、内容与内容元数据复用、内容加密。

- **内容与水印处理功能块**：非强制性处理步骤，该步骤对内容进行分析以产生内容跟踪（例如水印）元数据用于后续的下游处理，特别是用于区分（用相关源的信息来识别）这种元数据的过程。
- **元数据处理功能块**：管理和处理由内容提供商传递的与程序相关的元数据和使用权信息。
- **内容加密功能块**：完成受（扰码）保护的内容的加密，以便在内容传递过程中促进访问控制和机密性；对内容可实时加密，也可脱机预先加密（内容加密可以非强制性地支持无需解密的安全变码）。

注1 — 内容加密可在应用层的内容准备功能内实施。在某些情况下，作为一个选项，也可在内容传递功能内实施。

权利与密钥管理功能块：建立权利和密钥与内容之间的关联并管理将权利和密钥分发给终端设备中内容保护客户机功能块的过程。

内容保护客户机功能块：获得或接收权利和密钥，将此信息用于控制内容的解密和实施使用规则；该功能模块必须是防改动的。

内容传递功能：完成高速缓存和存储功能性并按照最终用户功能的请求传递内容；内容传递功能可以非强制性地处理（例如编码、加密）内容。

内容传递客户机功能：负责IPTV终端功能内的内容接收；完成内容媒体解密、去复用、解码和后续对内容的显示与存储处理（这些功能还必须具备防改动能力）。

- **水印检测功能块**：该模块若存在，则用于检测从服务提供商收到的内容中水印的使用，以验证或实施终端设备或终端设备的下游接口所需的内容使用规则。
- **水印嵌入功能块**：该模块若存在，则完成内容实例的区分，用于显示或后续的存储或重新分发。

权利源：始发涉及内容使用权的内容元数据。

内容源：始发需要汇总、处理和随后通过单收电视、电视点播之类的服务应用传递给最终用户的内容。

外置存储器功能块：接收后的内容存储机制，采用终端设备之外的物理设备且其存储和内容使用不受终端设备的管理。

注2 – 外部存储器若存在且其使用始终受终端设备的控制，则可以根据适用的终端设备合规性规则与稳健度规则被认为是经由受保护的授权接口的内置存储器。

7.4.3 服务保护架构功能和功能块

服务访问控制功能块：主要负责服务访问控制；该功能模块采用扰码和加密之类的使用安全机制来防止用户未经许可访问或获取服务。

服务访问控制客户机功能块：在客户机端完成与服务保护有关的任务，该任务由服务器端的服务访问控制功能块规定。

服务认证功能块：完成验证用户和/或终端设备真实性的认证；该模块也支持终端设备提出的对服务器进行验证的认证请求。

服务认证客户机功能块：除在客户机端完成与订户认证有关的任务之外，其功能还包括为相互认证而验证服务保护的服务器端的真实性。

8 安全机制

本建议书未规定任何具体的安全机制或解决方案，而是概括地描述了某些被认为可用于规定或实施涉及安全要求、安全架构功能实体和安全威胁的机制的安全机制。

下文所述的这套安全机制并未全面涉及上文列出的所有安全要求。

8.1 涉及内容保护的安全机制

内容安全机制包括在内容源与终端设备之间运行的一组功能，用于确保网络能够安全地分发（或传输）内容，确保最终用户能够安全地获取、消费、输出、存储和重新分发（或重新传输）内容。

内容安全机制可用于内容分发、内容获取、内容消费、内容存储、内容输出和内容重新分发。下述机制可用于满足IPTV内容和服务保护要求（所有要求都是非强制性的）：

8.1.1 内容加密

在许多情况下，可以对内容加密以防止内容在传递过程中遭到非法使用。

8.1.2 内容跟踪和标识

内容跟踪用于识别和跟踪内容的来源（源）和/或责任方（例如最终用户），为随后调查未经授权访问和使用内容的情况提供便利。

内容跟踪信息既可以作为元数据附在内容上，也可以作为取证水印附在内容上。内容跟踪水印通常应该是稳健的和无法察觉的，以避免有意或无意的删除。

建议采用视频签字技术来辅助内容标识。

8.1.3 加水印

加水印指通过改变某些内容特征在内容上添加信息的过程。该研究领域称为信息隐匿。

许多应用都很适合加水印，因为要从内容中删除该信息不那么容易。在IPTV服务中，加水印可以指直接在多路复用内容的视频流或音频流中加入隐藏的信息。理想情况下，水印是人的知觉无法看见或听见的，但经历媒体格式的转换后仍可完好地存在。

8.1.4 加内容标签

加内容标签是将描述内容性质的元数据插入到内容中或与内容产生关联，以及将内容方面与特性插入到内容中或与内容产生关联的过程。加了这种元数据标签的内容可以更容易地通过内容传递链上的中间设备进行存储、过滤或分类。

某些区域、某些主管部门或某些特定的IPTV部署可能要求提供某种类型的内容标签，如分级信息，以便让最终用户（订户）对他们认为不合适或有害的内容实施一定程度的访问控制。

8.1.5 安全的可变码方案

安全的可变码方案（STS）指能让中间网络节点在保留端对端安全的同时完成无需解密的变码的一种安全机制。这种机制可以通过同时进行可伸缩编码、渐进加密和分组而实现。

对于STS来说，实体有三种：发送方、中间网络节点和使用IPTV终端的用户。发送方完成安全的可变码功能以便从视频产生可伸缩的加密包，并把未加密的信息头加在该信息上。由中间网络节点读出未加密的信息头，并按照所需的变码操作用信息头所含的信息截短或丢弃多余的包，由IPTV终端对已加密的包进行解密并对明文包进行解码以产生视频。附录五对此做了详细描述。

注 — 本节并非要规定或描述附加的STS机制。该议题需要在其他建议书中进一步探讨。

8.2 涉及服务保护的安全机制

服务安全机制包括认证和授权。加密和解密系统之类具体访问控制机制的实施也包括在内。

8.2.1 服务认证

对于最终用户（订户）与服务提供商有直接关系的被管服务，服务提供商在提供服务之前通常会要求以安全的方式对终端设备和/或最终用户（订户）进行认证；此时，认证包括以安全的方式产生和显示能与服务提供商的订户数据库相关联的证书/信息，用于为了提供服务而验证终端设备和/或最终用户的真实性。

8.2.2 服务授权

在为了提供服务而对最终用户（订户）和/或终端设备进行认证之后，采用服务授权机制按照服务和订户提供条件进行授权并核准对具体的服务和其中驻留的内容的访问。

8.2.3 服务访问控制

在大多数情况（即便并非所有情况）下，服务保护系统将含有能够完成或者确实完成对服务控制信令业务量和内容业务量二者加密（扰码）和解密（解扰码）的机制。通常将在两个方向对双向服务控制业务量加密 – 从服务器到客户机和从客户机到服务器。另一方面，内容流通常只在从服务器（服务提供商）到客户机（终端设备）的方向加密。无论如何，总是存在从客户机到服务器上载内容流的使用方案，此时，可为了完成上载（例如为了确保只有得到认证和授权的服务提供商能够访问上载的内容）而在终端设备上对这样的内容加密 。

8.3 涉及网络的安全机制

本建议书未规定或描述任何涉及网络安全的机制。一般说来，预计核心网、接入网、承载网和传递网的实施可促进被认为是保护网络的运行完整性所需的机制的实施，比如说，包括拒绝服务（DoS）检测和预防。通常，IPTV服务提供商和终端设备所用的安全机制对这些网络是开放的，条件是这些安全机制在网络层提供的有效载荷数据要素层面运行或高于该层面运行。

8.4 涉及终端设备保护的安全机制

终端设备安全机制涉及的功能性范围很广，包括以硬件和软件两种方式实现的安全的和防改动的秘密数据存储、服务认证、服务授权、控制信号加密与解密、内容解密、内容权利元数据解码、内容使用的实施、水印检测与嵌入、程序性内容的认证与验证、服务和内容保护桥接与互换、数字输出端口（接口）加密、媒体路径防改动、可插拔和可更新安全处理器与部件等。

8.5 涉及订户或最终用户的安全机制

订户或最终用户安全机制主要与涉及隐私问题的或涉及最终用户机密性的信息的收集、存储和传输有关。这样，就可按照有可能获取、维护和重新使用该信息的收集点、终端设备和服务提供商来划分这些机制。因此可以预料，这些机制的描述和定义将纳入描述服务和终端设备安全的各节中。

有鉴于此，本建议书未规定订户或最终用户安全机制。可以预料，本建议书的下一步工作是进一步探讨这些议题。

关于订户安全的其他信息见附件A。

附件A

订户安全保护

（本附件是本建议书的组成部分）

A.1 用户隐私保护

在为普通用户提供IPTV服务时，充分考虑到安全性，订户数据保护是必不可少的。

订户数据可能还包括被跟踪数据信息，如变更频道前后的频道号、变更时间和EPG服务的用户信息、包的标识、播放时间等。上述信息具有个人和保密性质。防止所有这些订户数据不被滥用要求IPTV服务提供商考虑用户隐私保护问题。

- IPTV服务可以非强制性地处理传递IPTV服务所需的最小订户个人数据。
- IPTV服务在收集传递IPTV服务所需的信息之前可以非强制性地解释订户个人数据的预定用途并获得订户的同意。
- IPTV服务可以非强制性地销毁并非维持IPTV服务所必需的订户个人数据。
- 在服务提供商管理订户个人数据时，IPTV服务在严格保证安全的情况下可以非强制性地存储所收集的数据。

泄露订户个人数据的可能途径有多种：服务公司泄露，网络泄露，家庭泄露，例如通过终端设备。本建议书针对上述每一种泄露途径给出保护订户个人数据的方法。

为了防止泄露订户数据，建议IPTV服务提供商特别注意下面几个问题：

- 将订户个人数据分成需要控制和不需要控制两类。
- 安全地管理需要控制的订户个人数据。
- 确保需要控制的订户个人数据不用于预定用途之外的用途。

建议IPTV服务提供商特别注意下面几个在订户个人数据处理方面与服务和事务往来有关的问题。

- 将订户个人数据分成需要控制和不需要控制两类。
- 使用加密的通信信道传输需要控制的订户个人数据。

IPTV服务提供商有时要在终端设备中存储订户个人数据以提高服务效率。此时，建议IPTV服务提供商特别注意下面几个问题。另外，建议在终端设备交换信息时要考虑安全问题。

- 确保第三方无法轻易读取终端设备中存储的订户个人数据。
- IPTV服务提供商可以非强制性地控制对终端设备中存储的订户个人数据的访问。

- 确保终端设备中存储的订户个人数据能够由订户或服务提供商彻底删除。
- 要求不久之后终端设备最好能避免被计算机恶意软件（例如病毒和间谍软件）攻击。

A.2 家长控制，法定未成年人保护，访问控制

在IPTV平台上，可以用保护法定未成年人的机制来限制法定未成年人可访问的IPTV内容。从典型的使用情况看，IPTV服务的终端设备是由家庭中的多位成员共同使用的，包括法定未成年人。就终端设备而言，建议IPTV服务提供商：

- 确保必要时可由家长对内容设置分级。
- 确保能够按照家长设置的分级来操作终端设备。
- 确保能够在终端设备上更改家长的分级设置。
- 确保能够对终端设备实行密码控制，以便只有法定未成年人的监护人能够改变家长的分级设置。
- 确保能够按不同的年龄组设置内容分级。
- 确保能够按不同的年龄组划分订户的特权。
- 确保能够在终端设备上对法定未成年人观看某一特定频道或内容实现授权，例如采用PIN问询。
- 确保监护人不在法定未成年人近旁时能够在远端从网络备份存储器监视和接收为法定未成年人提供的内容。

注意，每一主管部门或区域在第三方组织方面的状况对消除有害内容可能是必要的，因为这关系到对内容流和访问的控制。人们可能会假定内容的原创者在内容制作时已充分考虑到广播内容有可能同时重新传输；因此充分注意传输延迟和分发成本的必要性也随之增加。

附录一

安全威胁

（本附录不是本建议书不可分割的组成部分）

本附录描述一组按照本建议书提出的某些要求或机制识别出的安全威胁。

已按照下述ITU-T建议书提出了安全威胁模型和其他基本资料：

- [b-ITU-T X.800]规定与安全有关的总体架构组成要素，可酌情用于开放系统之间的通信需要保护的情况。
- [b-ITU-T X.805]规定用于提供端对端网络安全的网络安全架构。

鼓励对与IPTV有关的安全问题感兴趣的各方阅读这些基础安全建议书；假定本建议书的读者了解此类建议书给出的信息。

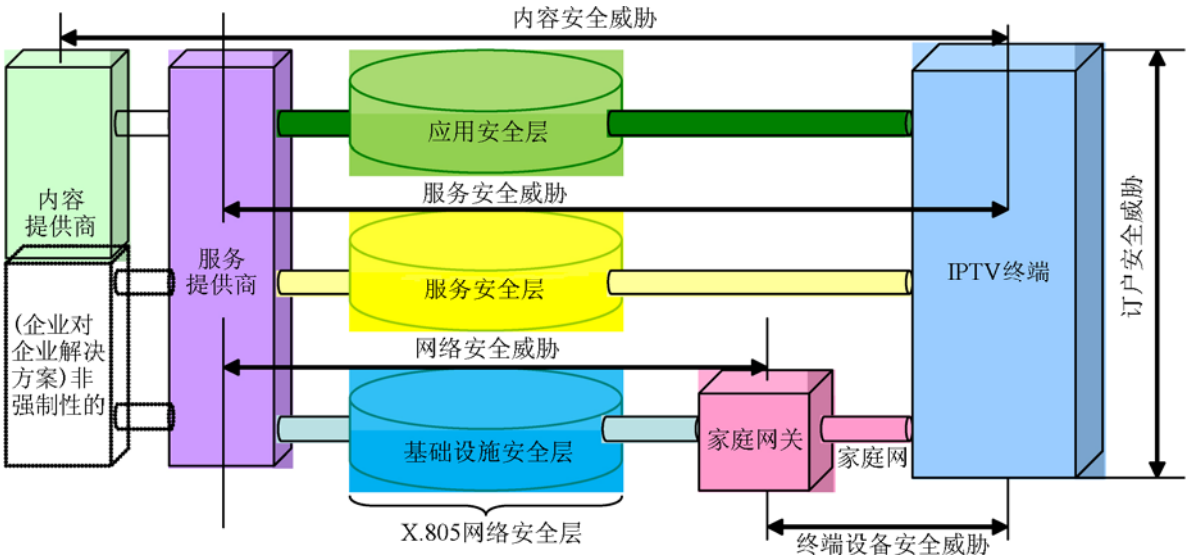
[b-ITU-T X.800]和[b-ITU-T X.805]确定了下述对网络的安全威胁（也成为IPTV适用的对服务和内容应用的安全威胁）：

- 销毁信息和/或其他资源。
- 破坏或更改信息。
- 盗窃、删除或丢失信息和/或其他资源。
- 泄露信息。
- 中断服务。

I.1 安全事件模型

对IPTV的安全威胁可分为下述几种类型：内容安全威胁、服务安全威胁、网络安全威胁、终端设备安全威胁和订户安全威胁。

图I.1说明了安全威胁模型，该图显示了这些安全威胁之间的关系。



图I.1 – 安全威胁模型

I.1.1 内容安全威胁

内容资产：属于内容提供商和/或服务提供商的资产；最终用户可通过终端设备消费该资产。

需要保护的内容资产包括：单收电视内容、VoD内容、推播式VoD内容、PVR内容、下载的应用程序等。

内容威胁如下：

- 拦截：通过非法监测提供服务的网络对数字内容机密性实施的破坏。
- 未经授权的收看。
- 未经授权的复制或重新分发。

I.1.2 服务安全威胁

服务资产：属于服务提供商的资产；包括媒体服务器、SCP服务器和运行信息，例如最起码包括服务日志和账务信息。

服务威胁如下：

- 侵犯 IPTV服务平台向订户提供的节目的版权。
- 冒名顶替/假冒IPTV服务提供商。
- 针对IPTV服务器（SCP服务器、媒体服务器等）的恶意威胁：可包括形成应用软件或通信协议安全泄露的黑客行为、拒绝服务攻击等。
- 盗窃（常常采用特洛伊木马之类的恶意程序）订户的信息（例如标识符信息、账务信息、租订信息）。

I.1.3 网络安全威胁

网络资产：属于网络提供商的资产；包括物理设备（例如路由器、交换机）和网络资源（例如带宽、多播服务等）。

网络威胁如下：

- 针对网络设备或资源（带宽）的故意威胁：对承载网的恶意攻击，如拒绝服务。

- 对IPTV承载网中所用的多播技术的安全威胁，如冒名顶替/假冒多播电视源或非法的多播组成员。
- 对内容分发网中节点的恶意攻击（例如DoS、黑客行为）。

I.1.4 终端设备安全威胁

终端资产：属于终端设备的资产，在IPTV服务中可由最终用户用于处理和存储内容及其他相关信息。

终端威胁如下：

- 通过改动设备硬件或软件而非法访问非加密内容；例如，通过拦截总线数据或通过SCP软件破解即可复制非加密内容。
- 利用软件破解或硬件改动非法获取密钥或访问设备中的其他秘密信息；攻击者可以改动设备存储器或分析数据流来获得密钥和其他秘密（内容密钥暴露导致内容泄露，设备密钥泄漏导致设备冒充）。
- 通过控制设备时钟系统之类的硬件方法禁用SCP系统的功能或通过安装病毒之类的软件方法耗尽设备的资源形成的设备功能失常。
- 在终端设备中下载、运行和存储未经授权的应用（例如软件程序）。
- 由来自网络的恶意代码/病毒引起的终端设备（硬件和软件）失效。
- 未经认证的终端设备连至家庭网。
- 订户未经授权的使用。

I.1.5 订户安全威胁

订户资产：属于订户的资产；包括关于订户、订户家庭、其IPTV事务往来等的信息。

订户安全要求实现内容安全的机制与实现服务安全的机制能够相互配合，因为IPTV服务中包括一种内容安全与服务安全相互配合的服务。

表I.1列出了订户威胁的示例。

表 I.1 – 订户安全的类别

	订户安全		
	服务实例	**威胁实例**	**保护机制示例**
内容安全	单收TV，VoD服务	非法复制	终端设备标识（服务保护、内容保护）
服务安全	双向服务	网页仿冒	个人标识（个人数据保护、PIN/口令）
	家长服务	欺骗	个人标识（PIN/口令、认证）
网络安全	未规定	窃听	用户线标识 加密数据、组播联合控制
终端设备安全	P2P服务	非法复制	内容保护（P2P）

附录二

SCP的互操作性

（本附录不是本建议书的组成部分）

II.1 SCP互操作性概述

可互操作的SCP方案有若干种：SCP-EE、SCP-B和SCP-IX。可互操作的SCP既可用于服务提供商域，也可用于最终用户域。本附录仅讨论终端侧。

II.2 可互操作的SCP方案

可互操作的SCP方案至少可分成三种模式： 端对端SCP（SCP-EE）、SCP桥接（SCP-B）和SCP互换（SCP-IX）。

1) 端对端 SCP (SCP-EE)

SCP-EE：两个或更多设备按照获得的权利采用单一SCP交换和访问内容。由于仅采用单一SCP，该模式是最简单的模式。

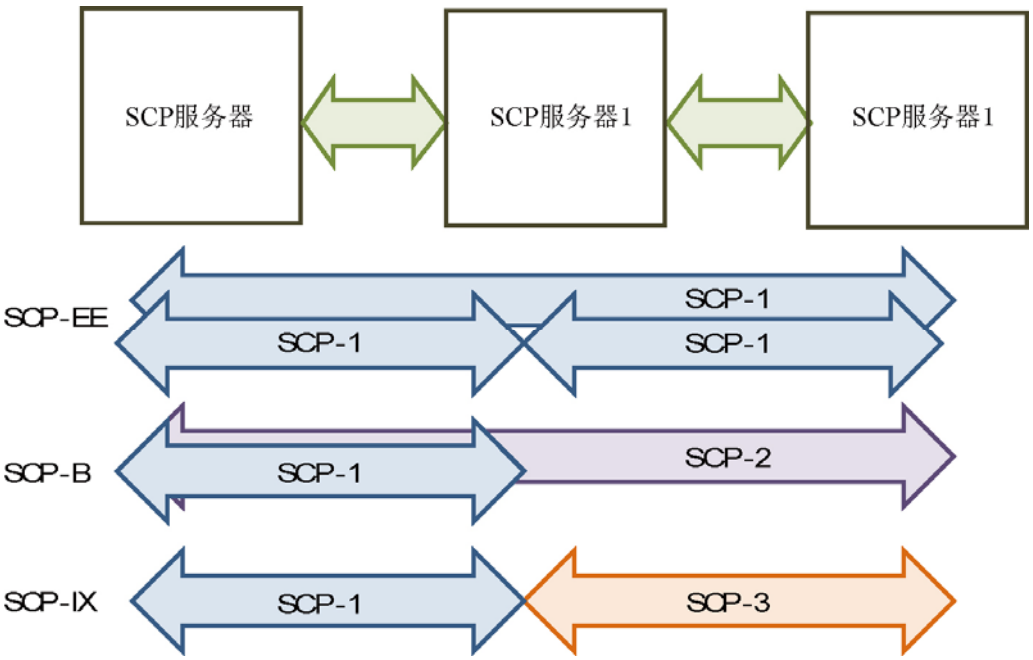
2) SCP 桥接 (SCP-B)

SCP-B：在单一的终端设备上部署了两个或更多SCP。经一个SCP系统（例如从网络）获取的内容能够按照获得的权利经驻留在同一设备中的另一个SCP访问。

3) SCP 互换（SCP-IX）

SCP-IX：这种情况可以用两个或更多设备来表征，其中每个设备都部署了一个或多个SCP。一个设备通过其SCP系统中的一个获取的内容能够按照获得的权利通过一个不同的SCP安全地转移到另一个设备或在另一个设备上访问。

图II.1说明了上述情况的一种模型。



图II.1 – SCP互操作模式

II.3 SCP互操作性的技术领域

下面几个领域表示 SCP-EE、SCP-B 和 SCP-IX 模式所需的关键互操作性要素：

1) 设备、用户和 SCP 的认证

在实体之间能够交换内容之前，必须安全地确定终端设备的标识符，可能还要确定其用户。另外，由于内容提供商可能不信任特定的*SCP*，有可能要在交换内容之前对*SCP*或实现的级别进行认证。这种认证应具备坚实的密码学基础，可采用各种广为人知的数字签字技术。特别是公开密钥密码术为认证协议提供了一种坚实的数字签字机制。

2) 权利表示交换

不同的*SCP*采用不同的权利表示语言或许可证格式。要让*SCP*-B和*SCP*-IX模式起作用，就需要一种共同的权利表示手段。该手段有可能采取通用权利表示语言（REL）或采取权利表示翻译器的形式。另一种可能的权利表示交换机制是许可证协商。

3) 内容交换所用的通用加密算法

要让内容安全地从一个*SCP*的控制之下转移到另一个*SCP*的控制之下或在不同物理设备上的同一个*SCP*之内转移，就需要对内容加密。该过程令内容无法使用，除非实体具有实施解密所需的相应的（若干）密钥。加密算法的类型繁多（例如块密码、流密码、基于公开密钥的密码等），但特别适合高速内容交换的一般都是采用对称密钥的算法。就互操作性而言，必须选择为数有限的达成共识的算法。最好还应具体规定一种默认算法。

4) 通用加密算法所用的密钥管理和/或交换

在内容交换能够安全地进行之前，经认证的实体有必要交换或共同产生用于特定实例的密钥。密钥管理通常是安全系统中最难实施的部分。公开密钥密码术之类的技术简化了设备密钥的分发，但却需要某种公开密钥基础设施（PKI）来建立和维护这些密钥的有效性。这种基础设施可由负责内容保护（而不是总体网络安全）的发证机构批准和维护。

5) SCP 客户机的安全下载

理想情况下，任何终端设备都能交换按照获得的权利从其他设备和/或采用任何*SCP*（合法地）获得的内容（即*SCP*-IX模式）。不过要注意，在制造时因市场力量而在每个终端设备中预装的每个*SCP*系统很难合乎实际需要；因此对于安全的机制而言，有必要下载并在终端设备上运行某个选定的*SCP*系统。安全的启动加载程序和安全的下载协议之类的要素在该互操作性领域发挥着一定的作用。

注 – 若在设备和端系统中部署了SCP互操作性，则IPTV设备应具备可信的架构以支持内容安全的互操作性。

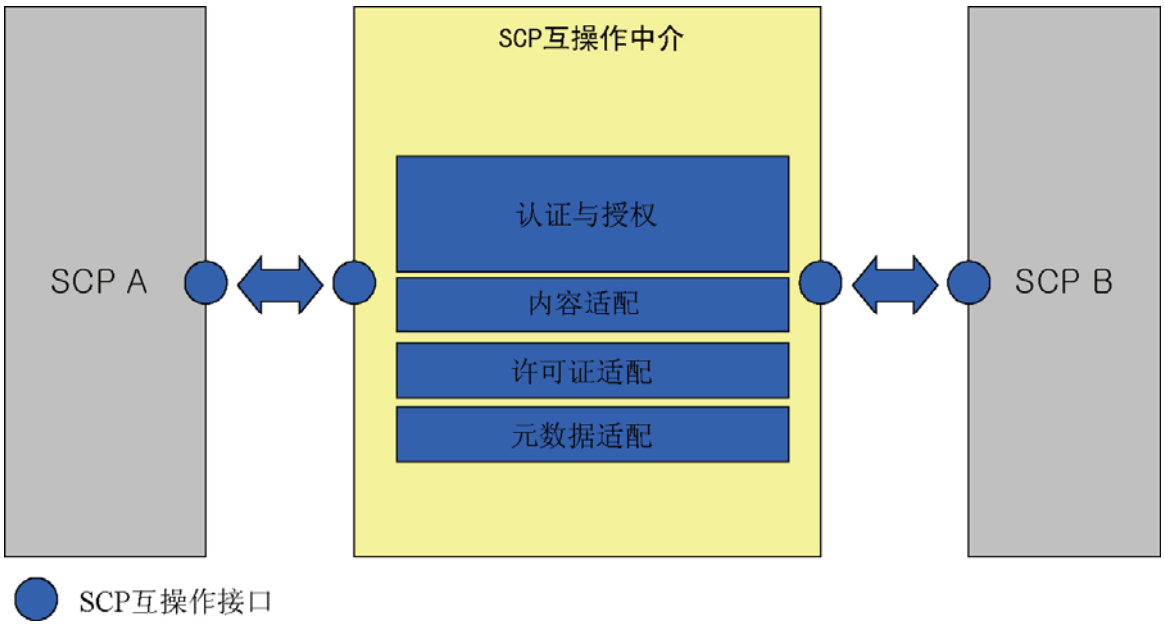
6) 安全的权利输出

为了安全地输出数字权利，IPTV SCP客户机应检查是否允许为SCP系统设定输出目标的使用权。数字权利可以做出能让目标SCP系统输出权利的权利表示。此时，IPTV SCP客户机应检查这些权利表示并授权适当的目标SCP系统输出数字权利。

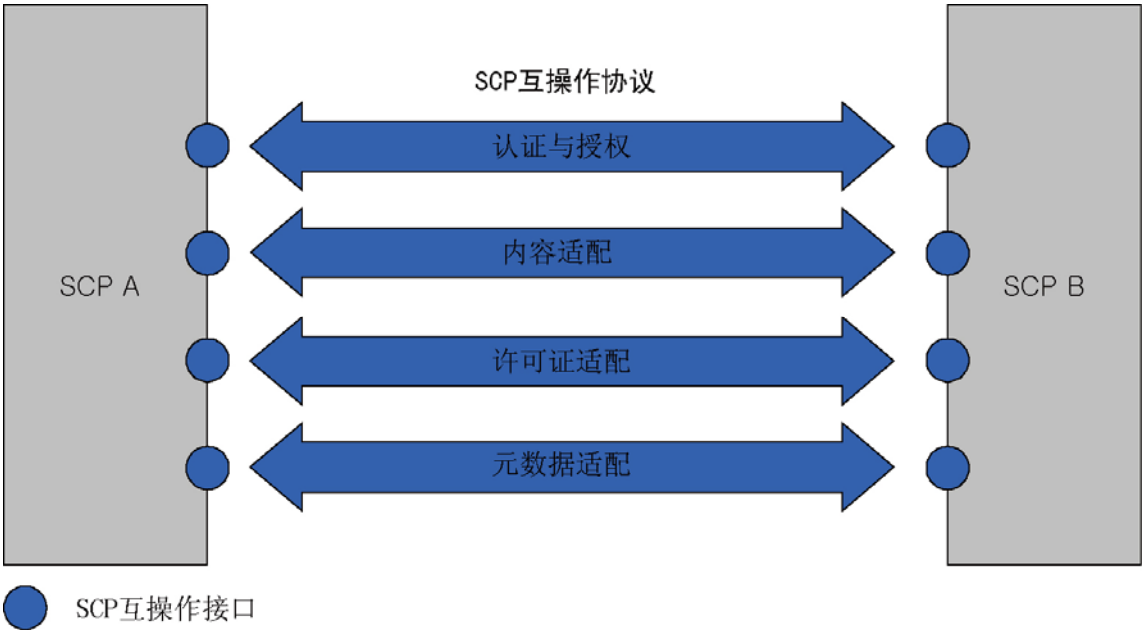
II.4 SCP的互操作架构

要考虑的SCP的互操作架构可能有两种。一种以基于中介的互操作性架构为基础，采用位于两个SCP系统之间的一个中介系统来处理互操作传输。另一种是基于标准协议的架构，采用标准的接口和协议来完成两个不同SCP系统之间受保护的数字内容及相关信息的转换。

图II.2和II.3表示了这两种可能的架构。



图II.2 - 基于中介的SCP互操作架构



图II.3 - 基于标准协议的SCP互操作架构

功能框说明：

- **内容适配**：内容适配负责转换密码算法。给出的几种预定的标准加密算法将有助于这些过程。
- **许可证适配**：许可证适配负责转换许可证。双方都熟知的任何临时许可证或标准许可证应维持与最初的许可证规定基本相同的许可性能（媒体资产与消费许可对）。许可证适配可包括一组权利映射（权利表示映射和语义映射）。另外，许可证适配也可负责重新分组权利信息并将其安全地传递给原有SCP客户机。
- **元数据适配**：元数据适配负责转换元数据信息。双方都熟知的临时元数据或标准元数据应维持与最初的元数据相同的信息。元数据适配可包括一组元数据映射（句法映射和语义映射）。另外，元数据适配也可负责重新分组元数据信息并将其安全地传递给另一SCP方。
- **认证与授权**：每一SCP方都应判断另一方是不是达到SCP互操作性的合适目标。这种判断通常伴随着相互认证过程，作为两个SCP方之间的一个预备性步骤。

特例：若SCP A和SCP B位于同一设备内，或两个SCP之间有专用的安全通信信道，则内容适配过程可不需要互操作处理。

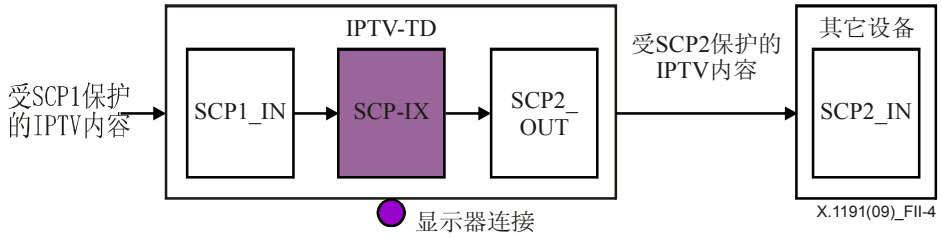
II.5 终端设备中部署SCP-B或SCP-IX的方案

本节描述要求服务安全与内容安全之间SCP互换的三种可能方案。

II.5.1 图中所用术语的定义

- SCP_IN：受SCP保护的IPTV内容借以进入的输入端口。
- SCP_OUT：受SCP保护的IPTV内容借以外出的输出端口。

II.5.2 方案1：采用SCP-IX的SCP

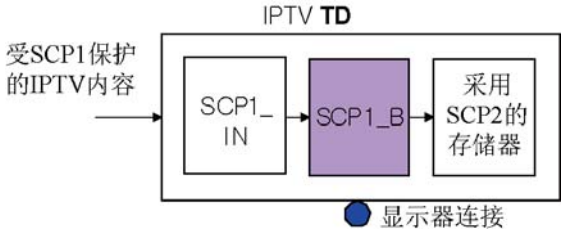


图II.4 - 采用SCP-IX的SCP

本例中的IPTV TD（终端设备）已采用SCP-IX的SCP来支持不带存储器的IPTV TD（仅采用特定的服务安全）与带存储器的外部设备（仅具备特定的内容保护）之间的互操作性。

为了支持与采用各种内容保护机制的任何种类的外部设备的安全和灵活的连接，对于两个设备之间的安全连接，IPTV TD应具备SCP-IX，而不是根据情况实施。

II.5.3 方案2：采用任选SCP-B和存储器的SCP



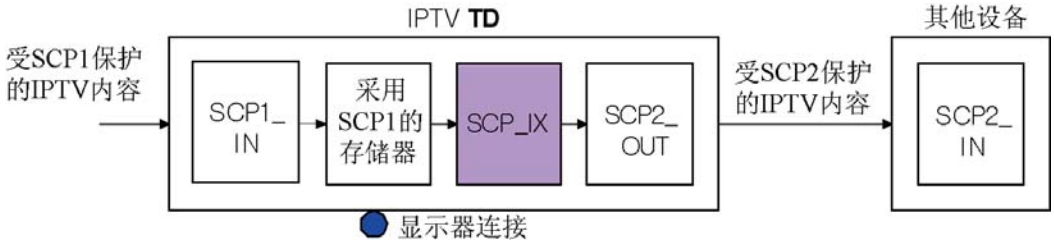
图II.5 - 采用任选SCP-B和存储器的SCP

本例中的IPTV TD已采用SCP-B的SCP支持同一设备上服务保护与内容保护之间的互操作性。

IPTV TD制造商可以将专有的内容保护机制用于内部存储器。此时，SCP_B不是必需的，存储器可采用SCP1。

为了支持与采用各种内容保护机制的任何种类的内部设备的安全和灵活的连接，对于服务保护与内容保护之间的安全连接，建议IPTV TD具备SCP_B，而不是根据情况实施。

II.5.4 方案3：采用存储器和SCP-IX的SCP



图II.6 - 采用存储器和SCP-IX的SCP

在本例中，IPTV TD以采用存储器和SCP-IX的SCP来支持内部内容保护机制与外部内容保护机制之间的互操作性。

为了支持与采用各种内容保护机制的任何种类的外部存储器的安全和灵活的连接，对于内部内容保护机制与外部内容保护机制之间的安全连接，建议IPTV TD具备SCP-IX，而不是根据情况实施。

附录三

IPTV内容保护过程实例

（本附录不是本建议书不可分割的组成部分）

下面描述VoD应用的一个示范性内容保护过程：

- 订户认证阶段
  - A 订户通过“服务和应用发现与选择客户机功能块”选择 VoD 应用。
  - “IPTV 应用功能”一收到请求，即发送给“应用协议子集功能块”以验证该订户。若验证成功，则将属于该订户的授权信息高速存储在 “应用协议子集功能块”内供查询。
- 内容选择阶段
  - 订户可以用从 ECG 获得的信息来选择特定的媒体内容，而“VoD 应用功能块”则将选定内容的位置信息（URL）传递给终端设备。
  - 终端设备中的“VoD 客户机功能块”接收内容位置并传输给“内容传递客户机功能”。
- 已加密内容传递阶段
  - “内容传递客户机功能”采用内容位置信息来请求（已加密）媒体内容；该功能还从“内容保护客户机功能块”请求与该内容相关的权利和密钥。
- 权利和密钥分发阶段
  - “内容保护客户机功能块”若不具备这种权利和密钥，则会向 IPTV 服务提供商的“权利与密钥管理功能块”请求这种权利和密钥。
  - “权利与密钥管理功能块”将申请“应用协议子集功能块”内与该订户有关的授权信息，以便采用该信息验证订户是否有权消费该内容。
  - 若验证成功，则将选定内容的权利和密钥分发给“内容保护客户机功能块”。
  - “内容保护客户机功能块”一收到密钥和权利，就转移给“内容传递客户机功能”，以便解密内容并控制其使用。

附录四

DVB内容保护与复制管理

（本附录不是本建议书不可分割的组成部分）

本附录概括了一组DVB内容保护与复制管理（DVB-CPCM）规范，这些规范由欧洲电信标准学会（ETSI）制定。

DVB-CPCM是全面标准化的系统的一个实例，该系统用于保护家庭网内和家庭网外电视和其他内容。DVB-CPCM可以从国际电联规定的（或其他的）IPTV服务保护机制获取内容，并在从获取到消费的整个内容生命周期内维持IPTV内容保护，包括受保护内容的存储、处理，以及在维持正当的授权使用的同时将受保护的内容输出到其他IPTV安全机制。

IV.1 引言

DVB CPCM是用于对传递给消费设备和家庭网的商业和免费（FTA）数字内容系统进行内容保护与复制管理的系统。CPCM对从CPCM系统获取内容到最终消费内容或按照该内容特定的使用规则从CPCM系统输出内容的内容使用过程实行管理。CPCM拟用于保护所有类型的内容，例如音频、视频以及相关的应用和数据。CPCM提出了在联网的消费设备的CPCM系统获取内容之后便于这些内容互操作性的规范，即可用于家庭联网，也可用于远端访问。该规范有些内容规定了满足技术合规性所需的信令和措施，另外一些内容解释了制定规范的理由，包括实施导则。参考模型提出了CPCM系统的框架，成为规范中其他部分的构成基础。

IV.2 定义

除正文中定义的术语外，本附录还定义了下列术语：

IV.2.1 Acquire 获取：内容从CPCM系统之外被接收并进入CPCM系统之内的动作。

IV.2.2 Acquisition Point (AP) 获取点 (AP)：用于发生内容获取的抽象CPCM功能实体。

IV.2.3 Acquisition 获取：内容从CPCM系统之外被接收并进入CPCM系统之内。

IV.2.4 Authorized Domain (AD) 授权域：由一个家庭的各成员拥有、租用或控制的一套合乎DVB CPCM的设备；一个家庭被认为是由作为同一住所的居住者而生活在一起的所有个体组成的一个社会单位（此处并未对家庭成员所拥有、租用或控制的设备的物理位置做任何假设）。

IV.2.5 Authorized usage 授权使用：得到允许的对CPCM内容的使用；由该内容适用的一组使用规则断言组成。

IV.2.6 Consume 消费：以可见形式给出内容或输出内容而排除任何其他用途的动作。

IV.2.7 Consumption Point (CP) 消费点 (CP)：用于完成消费的抽象CPCM功能实体。

IV.2.8 Consumption 消费：以可见形式给出内容或设备输出，其中含有旨在排除直接将内容转换为声音和图像之外的任何其他用途的一次转换或一个信号。

IV.2.9 Content item 内容项目：具有无限时长的内容的一个离散实例，例如节目/事件或其不完整片段。

IV.2.10 Content license 内容许可证：以安全的方式维护和交流的数据结构，含有管理CPCM内容项目的安全所必需的信息。

IV.2.11 Content 内容：CPCM系统要保护的数据；内容一般指视听内容，包括非强制性附带的数据，如字幕、图片/图形、动画、网页、文字、游戏、软件（包括源代码和对象代码二者）、脚本或要传递给用户供其消费的任何其他信息。

IV.2.12 Copy 复制：从已获取的内容或从原有的已存储内容项目生成一个新的已存储内容项目的CPCM管理过程。

IV.2.13 CPCM device CPCM设备：驻留了一个或多个CPCM实例的设备。

IV.2.14 CPCM system CPCM 系统：所有合乎规范的CPCM设备的集合。

IV.2.15 Device application 设备应用：CPCM 设备内的任何非CPCM功能性。

IV.2.16 Export Point (EP) 输出点 (EP)：CPCM内容借以离开CPCM系统的抽象CPCM功能实体。

IV.2.17 Export 输出：将受到CPCM系统明确保护和管理的CPCM内容释放到一个受控CPS、一个可信CPS或一个不可信空间。

IV.2.18 Move 移动：制作一个复制品，而原物则被移走、被擦除或无法继续访问的过程。

IV.2.19 Output 输出端：用于传输CPCM内容、供消费的内容或供输出的内容的设备接口或CPS。

IV.2.20 Processing Entity (PE) 处理实体 (PE)：处理CPCM内容的抽象CPCM功能实体。.

IV.2.21 Processing 处理：对已加密内容或未加密内容进行的不涉及消费或输出的合乎CPCM的操作，例如对CPCM内容进行可允许的转换以从其原有格式生成新的经转换的CPCM内容，或者从内容中提取音量或静像之类的信息。

IV.2.22 Usage State Information (USI) 使用状态信息 (USI)：表明授权使用每一CPCM内容项目的CPCM 内容元数据。

IV.2.23 View 观看：消费的动作；

注 – 这也包括收听纯音频内容的动作。

IV.2.24 Viewing 观看：消费；

注 – 这也包括收听纯音频内容。

IV.3 缩写词和首字母缩略语

除正文中的缩写词外，本附录还使用了下列缩写词：

AP 获取点

APECS 获取、处理、输出、消费、存储

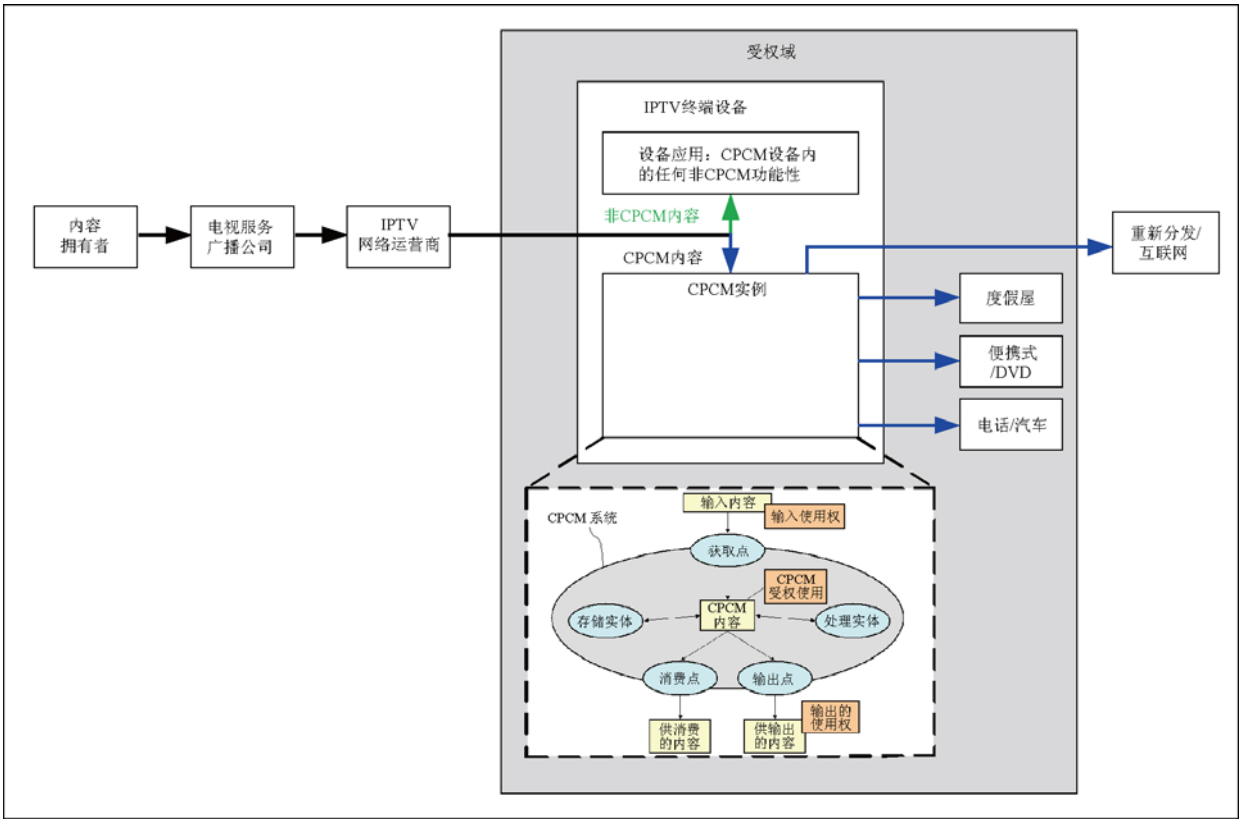
CL 内容许可证

CP 消费点

CPCM	内容保护与复制管理
CPE	客户端设备
CPS	内容保护系统
DVB	数字电视广播
EP	输出点
PE	处理实体
SE	存储实体
USI	使用状态信息

IV.4 CPCM架构

“授权域”（AD）位于CPCM的中心，是一个家庭拥有的设备的总称，即便设备不在家中也是如此。AD的概念认为，仅向一个机顶盒（TD）及与其相连的电视显示器中输入内容在网络娱乐时代是不够的。CPCM从一个可信源，例如作为终端设备的嵌入式设备或终端设备一部分的IPTV SCP系统中取出内容，并保护收到的内容流或内容文件，对如何收看、移动和复制进行管理。作为基础CPCM内容管理模型，供输入的内容进入CPCM系统而成为CPCM内容。CPCM内容在CPCM系统中受到管理和保护；该内容在遇到用户的消费或输出到另一个系统时离开CPCM系统。



图IV-1 - CPCM环境中的内容流程

CPCM支持家庭网上内容的多种使用方案；它还可在远端管理对内容的访问，例如通过宽带互联网连接上的笔记本计算机。采用CPCM，服务提供商可以通知设备制造商对于每种内容可允许的使用方案。这样就拓展了当今使用的许多保护方法，如IPTV SCP 技术中嵌入的方法，这种技术通常限于内容源设备（例如机顶盒）与数字显示设备之间单一的点对点互联线路。

CPCM则超越了这种本地化的保护，为广播公司、网络运营商和内容拥有者提供了一个选项，允许某个家庭成员在出差旅行或度假期间从饭店之类的远端进行访问。

CPCM还能够让用户将内容复制到便携式设备或DVD光盘之类的可更换存储器上。只要播放设备属于同一授权域，该设备就能够播放内容，即便设备从家中断开或与原来的服务提供商断开。CPCM内容将设备添加到授权域或从中删除都不需要服务提供商在线授权。

CPCM内容保护系统不是一个独立的实体；它被插入/叠加到整体端对端IPTV SCP分布系统中。它就这样与IPTV SCP系统共存，而不是替代IPTV SCP系统。在任何终端设备中，CPCM实例都是非强制性的；但它若不存在，则不允许终端设备访问任何受CPCM保护的内容。尽管如此，终端设备并非有必要实施所有的CPCM要素。需要的只是那些对终端设备有用的要素，以完成终端设备所需的功能性。例如，一个简单设备若没有CPCM存储和输出要求，可能仅实施CPCM获取和消费功能性。

IV.5 CPCM参考模型与功能实体

CPCM参考模型规定一组五个抽象内容管理功能，涵盖了消费环境中所有相关的内容使用方案：获取、存储、处理、消费和输出。这些功能映射至五个CPCM功能实体：获取点、存储实体、处理实体、消费点和输出点。图IV-1按照这组抽象功能实体显示了CPCM系统的一种视图。

因此，通过在某个CPCM设备中实现这种获取点，供输入的内容就凭借在该获取点的获取功能进入CPCM系统而成为CPCM内容。CPCM内容可由CPCM设备中实施的相应的功能实体（存储实体、处理实体）来存储或处理。CPCM内容在遇到消费点的消费或输出点的输出时离开CPCM系统。另外，这些功能实体可在任何CPCM 设备内实施。

IV.6 CPCM授权域

CPCM设备在逻辑上可以划归授权域。若所有这些设备都属于一个家庭，则这些设备就构成了该家庭的授权域（AD）。因此，授权域为映射到单一家庭边界的内容提供了一个目的地。一般说来，AD可以视为属于一个家庭的所有CPCM设备、位于主要住所的设备、位于另一住所（例如度假屋）的设备、仅用于间断地与上述固定设备连接的便携式手持设备或固定在属于该家庭的车辆上的设备的逻辑分组。AD拟用于设备的自主逻辑分组；它不需要任何外部管理。不过要注意，可能会出现AD连接到某个特定服务提供商的情况，该服务提供商可能试图支配AD作为向客户提供的服务的一部分。

IV.7 CPCM内容使用规则

对任何CPCM内容项目的授权使用指一套使用规则断言，并在与内容绑定的CPCM使用规则中表示。CPCM使用规则可以由内容提供商或服务提供商设定，或由传递形式（例如免费广播）映射而来。存储、消费和输出操作的可执行范围可能隶属于内容的授权使用。CPCM规定了一套通用的使用规则，对于CPCM系统中的内容，任何内容提供商都相应地能够从这套规则中选择或能够推导出所需的授权使用。对于客户而言，设定CPCM使用规则旨在特别灵活地涵盖所有适用的内容保护和管理模型，以及特别简明地维护明确和比较简单的内容使用模型。

IV.8 使用状态信息元数据

某一内容项目的授权使用被编码为CPCM内容元数据，称为使用状态信息（USI）。CPCM内容是按照每一内容项目所适用的USI来管理和保护的。由CPCM系统间接完成的合乎规范的USI状态跃迁除外，对CPCM系统中的内容持有合法授权的实体可以在CPCM系统获取内容之后对内容项目的USI状态执行其他更改。

IV.9 CPCM内容

“内容”一般指视听内容，还包括非强制性附带的数据，如字幕、图片/图形、动画、网页、文字、游戏、软件（包括源代码和对象代码二者）、脚本或要传递给用户供其消费的任何其他信息。CPCM内容指受到CPCM系统管理和保护并符合CPCM系统的内容。内容项目是具有无限时长的内容的一个离散实例。每一CPCM内容项目都附带内含相关USI的内容许可证信息以及其他更多的CPCM元数据。CPCM系统能够视USI所需的目标功能性和/或使用规则的实施情况以不同的方式处理内容许可证和内容项目本身。

IV.10 CPCM设备

CPCM设备是以合乎规范的方式实施任何CPCM功能性的设备。CPCM功能性的实施被认为是一个CPCM实例。CPCM设备是驻留了一个或多个CPCM实例的设备。除CPCM功能性之外，CPCM设备还可以含有其他非CPCM合规功能。CPCM内容处理只由设备内的CPCM实例完成。设备的非CPCM部分无法访问CPCM内容。CPCM设备还可以驻留从其他保护系统安全地获取内容所用的或安全输出（也有可能是消费）CPCM内容所用的非CPCM安全功能性。

IV.11 使用规则与使用状态信息

CPCM中的一条使用规则就是对CPCM系统内欲受控的内容的一种特定操作或行为。用于某一特定CPCM内容项目的一组完整使用规则断言被称为对这种CPCM内容项目的授权使用。内容项目的授权使用被编码为该内容项目的使用状态信息（USI），也就是表明对该特定内容的授权使用的CPCM内容元数据。

附录五

安全的可变码方案

（本附录不是本建议书不可分割的组成部分）

V.1 安全的可变码方案概述

由于各种类型的设备日渐流行，如PDA、非PC设备、蜂窝移动电话和智能移动终端，内容的变码引起了越来越多的注意。变码指将图像、文本、音频和视频之类的内容从原有格式转换为另一种不同格式或质量的过程。

变码功能力图减小调制解调器链路和无线接入链路之类的窄带宽接入链路上多媒体内容的下载延迟，并解决客户机设备支持的编码格式与多媒体内容提供商所用的编码格式之间的失配问题。变码功能还让受计算能力限制的终端能够根据变码能力显示已编码的内容。

对于安全的可变码方案来说，实体有三种：发送方、中间网络节点和使用IPTV终端的用户。变码功能驻留在位于内容提供商与客户机设备之间的中间网络节点中。变码架构有两种：传统的变码架构和安全的变码架构。

在传统的变码架构中，将变码代理用做位于内容服务器与客户机设备之间的中间网络节点。发送方对内容进行充分压缩并加密，然后将已加密的内容发送给称为变码代理的中间网络节点。变码代理对已加密的内容进行解密并解压缩。然后变码代理改变内容的大小或其格式，进行新的压缩，最后对变码数据重新加密，以传输给客户机设备。客户机设备对已加密的内容进行解密并采用新的压缩算法对内容解压缩。不过要注意，变码代理出现了安全问题，即一旦变码代理在内容加密之前对内容进行了解密，则未加密的内容会驻留在变码代理中。换句话说，旁观者可以通过窃听而访问未加密的内容。这种未加密的内容削弱了对隐私的端对端安全保证，因为应该只有发送方及合法客户机可访问处于未加密状态的内容。

为了解决安全问题，提出了一种安全的变码架构。安全的变码方案就是一种在保持端对端安全的同时可让中间网络节点无需解密而完成变码的安全方案。该安全方案能够通过同时执行可伸缩编码、渐进加密和分组来完成。发送方完成安全的变码功能以便从视频产生可伸缩的加密包，并把未加密的信息头加在该信息上；由中间网络节点读出未加密的信息头并按照所需的变码操作用信息头所含的信息截短或丢弃多余的包，由IPTV终端对已加密的包进行解密并对明文包进行解码以产生视频。

参考资料

[b-ITU-T H.222.0] ITU-T H.222.0建议书 (2006年)，| ISO/IEC 13818-1:2007，《信息技术-动态图像和伴音信息的通用编码：系统》（*Information technology – Generic coding of moving pictures and associated audio information: Systems*）。

[b-ITU-T H.622.1] ITU-T H.622.1建议书 (2008年)，《支持IPTV服务的家庭网络架构和功能要求》（*Architecture and functional requirements for home networks supporting IPTV services*）。

[b-ITU-T M.1400] ITU-T M.1400建议书 (2006年)，《运营商的网络间互连的标志》（*Designations for interconnections among operator's networks*）。

[b-ITU-T Q.1290] ITU-T Q.1290建议书 (1998年)，《智能网定义中使用的术语表》（*Glossary of terms used in the definition of intelligent networks*）。

[b-ITU-T X.800] ITU-T X.800建议书 (1991年)，《用于CCITT应用的开放系统互连安全架构》（*Security architecture for open systems interconnection for CCITT applications*）。

[b-ITU-T X.805] ITU-T X.805建议书 (2003年)，《提供端到端通信的系统的安全架构》（*Security architecture for systems providing end-to-end communications*）。

[b-ITU-T Y.101] ITU-T Y.101建议书 (2000年)，《全球信息基础设施术语：术语和定义》（*Global Information Infrastructure terminology: Terms and definitions*）。

[b-ITU-T Y.1901] ITU-T Y.1901建议书 (2009年)，《支持IPTV服务的要求》（*Requirements for the support of IPTV services*）。

[b-ITU-T Y.2012] ITU-T Y.2012建议书 (2006年)，《NGN版本1的功能要求和架构》（*Functional requirements and architecture of the NGN release 1*）。

[b-ETSI TS 102 825] ETSI TS 102 825（全部），数字视频广播（DVB）；内容保护和复制管理（DVB-CPCM）*Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM)*.
<http://pda.etsi.org/pda/AQuery.asp>

[b-ATIS 0800001] ATIS 08000001，《IPTV DRM互操作性要求》（*IPTV DRM Interoperability Requirements*），电信行业解决方案联盟IPTV互操作性论坛（*ATIS-IIF*），2007年4月。
<https://www.atis.org/docstore/product.aspx?id=21212>

[b-ATIS 0800006] ATIS 0800006，《IIF缺省加扰算法（IDSA）IPTV互操作规范》（*IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification*），2007年2月。
<https://www.atis.org/docstore/product.aspx?id=22663>

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	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、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	电缆和外部设备其他组件的结构、安装和保护
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	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
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、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况

瑞士印刷
2009年，日内瓦