

国际电信联盟

**ITU-T**

国际电信联盟  
电信标准化部门

**J.1010**

(09/2016)

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

有条件的接入和保护 – 可交换的嵌入条件  
接入与数字版权管理方案

---

**用于可交换条件接入/数字版权管理 (CA/DRM)  
解决方案的嵌入式通用接口(ECI)；使用案例和  
要求**

ITU-T J.1010 建议书



# ITU-T J.1010 建议书

## 用于可交换条件接入/数字版权管理（CA/DRM） 解决方案的嵌入式通用接口（ECI）； 使用案例和要求

### 摘要

ITU-T J.1010建议书具体列出用于可交换条件接入/数字版权管理（CA/DRM）的嵌入式解决方案的使用案例和要求，从而有利于可以接收广播和宽带内容的用户端设备（CPE）在可信任环境中下载CA/DRM客户端。通过使用可下载的多CA/DRM服务，消费者有权消费由DRM和/或条件接入系统（CAS）控制的广播和宽带内容，尽管从可信任来源下载到不同类型的CPE时，CPE并没有所需的内容相关CA/DRM客户端（其中包括机顶盒（STB）、智能电视、个人电脑、智能手机和/或智能平板电脑）。

### 历史沿革

| 版本  | 建议书名称        | 批准日期       | 研究组 | 唯一标识*                                                                     |
|-----|--------------|------------|-----|---------------------------------------------------------------------------|
| 1.0 | ITU-T J.1010 | 2016-09-02 | 9   | <a href="http://handle.itu.int/11.1002/1000/12772">11.1002/1000/12772</a> |

### 关键词

CA/DRM、可交换嵌入式通用接口、零售CPE

\* 欲查阅此建议书，请在网络浏览器的地址字段内输入URL <http://handle.itu.int/>，然后再输入该建议书的唯一ID，例如：<http://handle.itu.int/11.1002/1000/11830-en>。

## 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/>。

© 国际电联 2017

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

# 目录

|                                     | 页码 |
|-------------------------------------|----|
| 1 范围 .....                          | 1  |
| 2 参考文献 .....                        | 1  |
| 3 定义 .....                          | 1  |
| 3.1 其他地方定义的术语 .....                 | 1  |
| 3.2 本建议书定义的术语 .....                 | 1  |
| 4 缩略词和首字母缩略语 .....                  | 2  |
| 5 惯例 .....                          | 2  |
| 6 可交换CA/DRM嵌入式解决方案的要求.....          | 3  |
| 6.1 概述 .....                        | 3  |
| 6.2 一般性要求 .....                     | 4  |
| 6.3 多用途相关要求 .....                   | 5  |
| 6.4 实用性相关要求 .....                   | 5  |
| 6.5 ECI客户端交换相关要求.....               | 5  |
| 6.6 ECI系统安全相关要求.....                | 6  |
| 附件A – 使用案例.....                     | 8  |
| A.1 使用案例1 .....                     | 8  |
| A.2 使用案例2 .....                     | 8  |
| A.3 使用案例3 .....                     | 9  |
| A.4 使用案例4（与可信第三方（TTP）有关的使用案例） ..... | 9  |
| 参考文献.....                           | 10 |

## 引言

条件接入（CA）和数字版权管理（DRM）实现的服务和内容保护对于高速发展的数字广播和宽带，包括内容、服务、网络 and 用户端设备（CPE）至关重要，以便对内容所有者、网络运营商和付费电视（PayTV）运营商的商业模式提供保护。一方面，CA在理念上侧重于获取服务提供商利用网络传播的受保护内容的机制，另一方面DRM按照用户合同主要用来阐述使用权的类型和范围。

PayTV运营商建立了实施基本功能标准并增加了专有元素的数字电视平台。多数用于传统数字广播、IPTV或新的OTT（置顶）服务的CA和DRM系统通过结合专有要素捕获用户端设备（CPE）。因此，为网络或平台A配置的用户端设备无法用于网络或平台B，相反亦然。为此，由于各国规范不同，平台各异，数字电视的消费市场依然处于分割状态。可接插CA/DRM模块仅提供了部分解决方案：这些模块对于CA/DRM系统而言仍具专有性，且价格不菲，主要用于有线或卫星电视。由于缺少适当的物理接口，不适用于平板电脑等现代设备。

目前采用的解决方案，无论是嵌入式或接插硬件均产生“锁定”效果。这种情况严重限制了数字多媒体内容市场中许多企业的自由发展。随着技术的进步，创新型软件CA/DRM解决方案应运而生。这些方案在最大程度上实现了互操作性的同时保持高度安全性，为满足市场未来需求带来希望，为新企业提供了机遇并扩大了消费者选择。

消费者在搬家或更换网络提供商，甚至使用了不同商用视频门户的服务设备后可继续使用已购置的CPE符合消费者的利益。这只能通过CPE在适当的安全架构基础上确保实现CA和DRM之间的互操作性。防止CPE市场的进一步分割并促进竞争必须确保CA和DRM系统具有方便消费者和有利于环境的可交换性。

## 用于可交换条件接入/数字版权管理（CA/DRM） 解决方案的嵌入式通用接口（ECI）； 使用案例和要求

### 1 范围

新建议书草案的目的是为可交换嵌入式通用接口确定一套基本要求，以便将必要的CA/DRM系统下载至CPE。下载程序是在可信任的环境下操作的，为采用不同终端设备依照最终用户获得的内容权利消费通过广播和/或宽带连接提供的受保护内容创造条件。本建议书是规范整体ECI生态系统的系列建议书之一。

### 2 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或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。

应用本文件需参考以下文件：

[ETSI GS ECI 001-1] ETSI GS ECI 001-1：用于可交换条件接入/数字版权管理（CA/DRM）解决方案的嵌入式通用接口（ECI）；第1部分：架构、定义和概述。

[ETSI GS ECI 001-2] ETSI GS ECI 001-2：用于可交换条件接入/数字版权管理（CA/DRM）解决方案的嵌入式通用接口（ECI）；第2部分：使用案例和要求。

### 3 定义

#### 3.1 其他地方定义的术语

无。

#### 3.2 本建议书定义的术语

本建议书定义了下列术语：

**3.2.1 嵌入式通用接口（ECI）：**ETSI ISG“嵌入式CI”规定的架构和系统可使用户端设备基于软件的可交换ECI客户端得到开发和实施，由此提供用于ECI的CPE设备互操作性。

**3.2.2 嵌入式通用接口客户端（ECI客户端）：**实施符合规划的嵌入式CI规范的CA/DRM客户端。请注意，为在保护方式下收到消费者有关内容传播方或运营商传播的内容的权利和版权提供各种手段的是CPE中的软件模块。该模块还接收消费者可享有的版权或权利条件以及解密不同电文和内容的密钥。嵌入式CI客户端可能拥有一个相关智能卡。

**3.2.3 嵌入式通用接口（ECI）主机：**CPE硬件和软件系统涵盖ECI相关功能并与ECI客户端相连接。请注意，ECI主机是CPE固件的一个组成部分。

**3.2.4 受保护的内容：**通过线性或非线性传送手段向用户应用传送的所有各类受保护的媒体，尤其是A/V和相关元数据。

**3.2.5 软件包：**与主机和客户端相连接的一组软件接口将CA/DRM客户端与主机严格分离。接口的提供使CA/DRM客户端之间的互换成为可能。

## 4 缩略词和首字母缩略语

本建议书采用下列缩略词和首字母缩略语：

|        |                |
|--------|----------------|
| AES    | 先进的加密标准        |
| CA     | 条件接入           |
| CA/DRM | 条件接入/数字版权管理    |
| CE     | 消费电子           |
| CPE    | 用户端设备          |
| CSA    | 通用扰码算法         |
| DECE   | 数字娱乐内容生态系统     |
| DRM    | 数字版权管理         |
| DVB    | 数字视频广播         |
| ECI    | 嵌入式通用接口        |
| IP     | 互联网协议          |
| IPTV   | 使用互联网协议（IP）的电视 |
| OMA    | 开放移动接入         |
| OTT    | 置顶（通过开放式互联网）   |
| PVR    | 个人录像机          |
| TTP    | 可信任第三方         |
| URI    | 使用权利信息         |
| VM     | 虚拟机器           |

## 5 惯例

在本建议书中：

关键词“**需**”（**is required to**）指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“**建议**”（**is recommended**）指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“**禁止**”（**is prohibited from**）指必须严格遵守的要求，如果要宣称符合本文件，就不得违反。

关键词“可作为选项”（**can optionally**）指允许可选的、但并非建议遵守的要求。该术语并非旨在暗示销售商的实施必须提供该选项且该功能部件可作为选项由网络运营商/业务提供商激活，而是指厂商可作为选项提供该功能部件并仍根据规范宣称符合本文件。

在本文件正文及其附件中，有时会出现“须”（shall）、“不得”（shall not）、“应”（should）、“可”（may）等词语。在这些情况下，这些词语应分别理解为“需”、“禁止”、“建议”和“可作为选项”。在附录或标为“用于通报情况”的材料中出现这些短语和关键词应理解为并非出于规范性的意向。

## 6 可交换CA/DRM嵌入式解决方案的要求

### 6.1 概述

本文件涉及的**ECI**基本要求综合规范是规定基于软件的、通用嵌入式和可交换CA/DRM系统架构多项工作成果的组成部分。上述系统是解决市场分割并实现互操作性最适宜并具前瞻性的解决方案。计划采用的内容安全方式具有以下关键优势：

- 基于软件的实施带来的灵活性和可扩展性
- 满足未来需求的解决方案和有利于创新的可交换性
- 对通过包括OTT在内的广播和宽带传送内容的适用性
- 对多屏幕环境的支持
- 通过避免“锁定”对平台运营商、网络/服务提供商和消费者市场提供激励。
- 规范促进市场发展的开放式生态系统

**ECI**系统旨在在所有相关层面和方面实现CPE中CA和DRM系统的可交换性，为消费者带来最低成本并在最大程度上减少对CA或DRM厂商在PayTV市场目标产品开发中的限制。因此，除其它功能外，**ECI**具有以下功能：

- CA软件包分别具有DRM核（以下简称**ECI客户端**）并具有：
  - CPE所有相关功能的标准化接口；
  - 可运行的标准**虚拟机（VM）**。
- 支持无智能卡系统以及基于智能卡的系统。
- CPE中包含多个此类软件包，每个软件包运行在自己的**VM**之上。
- 利用安全标准化负载理念独立于其它CPE软件安装的**ECI客户端**。
- **先进的安全性**，亦称为芯片集安全性，支持软件保护并防止非授权内容接入。
- 用户发现**ECI客户端**下载权利的方法。
- 取消**ECI客户端**（部分）功能和CPE功能的方法。
- 适用于传统数字广播、IPTV或现代OTT系统。

尽管**ECI**显示出与已部署解决方案的相似性，但差别依然显著：

- 1) 模块采用软件形式，而不是硬件形式，因此消费者转换为CA或DRM系统无需增加成本。
- 2) 可在同一个CPE中实施若干并行的**ECI客户端**，无需增加相关成本。
- 3) 这些客户端可同时运行于一个设备。

因此，CA或DRM组件可以更为简便地交换，使最终用户得以更换运营商或通过其CPE获得不同的运营商服务，无需更换昂贵的模块。

由多个部分组成的完整工作成果包括一组规范，其中包括有关使用案例和要求的综合规范以及以下各项规范：

- 第1部分：架构、定义和概况[ETSI GS ECI 001-1]
- 第2部分：使用案例和要求[ETSI GS ECI 001-2]
- 第3部分：CA/DRM包、负载软件、接口、取消[b- ETSI GS ECI 001-3]
- 第4部分：虚拟机器（VM）[b- ETSI GS ECI 001-4]
- 第5部分：先进的安全系统[b- ETSI GS ECI 001-5]
- 第6部分：信任环境[b- ETSI GS ECI 001-6]
- 第7部分：扩展要求[b- ETSI GS ECI 001-7]

这些规范综合阐述了最终用户提出要求时通过下载**ECI客户端**随时更换**ECI客户端**的解决方案。**ECI客户端**安装在标准软件包中，它使用不同承载软件，利用单独的安全算法并独立于CPE中所有其它软件保护**ECI客户端**的完整性并防止替换攻击密钥。软件包与CPE的接口为通用接口（定义见GS ECI 001-3 [b- ETSI GS ECI 001-3]），使**ECI客户端**与CPE中各种功能和其它功能的互动成为可能。

**ECI客户端**运行于虚拟机器的情况见GS ECI 001-4 [b- ETSI GS ECI 001-4]中的定义。

GS ECI 001-5 [b- ETSI GS ECI 001-5]规定了保护在CPE处理器芯片内容解密设施内穿行的内容密钥的先进安全机制。

本文件涉及的使用案例和要求将作为实施CPE中可互操作CA/DRM系统的基础。

**ECI**规范仅适用于条件接入和/或数字版权管理系统控制的、经服务提供商扰码的内容接收和进一步处理。条件接入和/或DRM系统未控制的内容不在本文件范围之内。

**ECI**综合规范旨在通过**信任机构**的控制与合同框架（许可协议）、合规和稳健规则以及适当的认证程序（见注释）联合使用（见GS ECI 001-6 [b- ETSI GS ECI 001-6]）。

适合**ECI**的CA/DRM系统的端对端安全不仅需要技术规范。**ECI**技术是**ECI**合规生态系统的一项要素（见GS ECI 001-1 [ETSI GS ECI 001-1]）。端对端安全是由信任机构在考虑到法律框架、设备认证和其它问题的情况下建立的。以下要求基于附件A给出的使用案例。

## 6.2 一般性要求

[R 01] **嵌入式CI**须适用于任何广播、宽带和混合（广播和宽带）服务，通过任何适当的接入网类型向任何适用设备类型提供保护内容。

- [R 02] **嵌入式CI**须定义ECI核软件和紧密关联的CA/DRM软件功能的**软件包**，与CPE其余软件要素明确分离。
- [R 03] **嵌入式CI**须提供可与当今最先进CA/DRM系统提供的安全功能相当的增强性安全功能。
- [R 04] **嵌入式CI**须能在5年期限内实现对可在各类情况下长期运行并维护的安全CA/DRM系统的设计。

### 6.3 多用途相关要求

- [R 05] **嵌入式CI**须支持在一个CPE中采用一个以上的CA/DRM客户端，支持并行处理至少两个不同的**受保护内容**事件。
- [R 06] 相关架构须实现某个CPE中的不同ECI客户端可相互识别，可相互建立信任并可在两者间传送内容和相关**URI**。
- [R 07] 相关架构须实现**ECI客户端**可建立至其所连接**ECI主机**的信任关系并可向**ECI主机**安全传送**URI**。
- [R 08] **嵌入式CI**须确保满足各国法律和监管要求，如数据隐私保护和保护未成年人。
- [R 09] **嵌入式CI**须支持向某个家庭域或家庭网中的其他终端（包括移动终端设备）导出法律要求的**受保护内容**。这意味着相关架构提供必要的接口，使得CPE中的ECI客户端可与同一设备中的另一个ECI客户端对话。只有符合相关内容所有人发布的使用权限后才可如此。
- [R 10] ECI客户端的实施可向非ECI设备导出**受保护内容**。只有符合相关内容所有人发布的使用权限后才可如此。

### 6.4 实用性相关要求

- [R 11] **嵌入式CI**须为用户接口的实施提供API，实现很高的可用性和用户交互的便捷处理。
- [R 12] 相对于可比较的CA/DRM解决方案，即使受影响的两个信道（业务）采用不同的CA/DRM制式，**嵌入式CI**也不应增加明显的时延。应注意，并不假定在正常的信道（业务）变更期间，须交换CA/DRM制式。
- [R 13] 所有ECI相关活动（如正常操作、下载**ECI客户端**）不应对用户体验和性能带来明显影响。

### 6.5 ECI客户端交换相关要求

- [R 14] **嵌入式CI**须允许在无须征得CA/DRM生产商、设备制造商、平台或业务运营商同意的情况下变更到一个新的业务提供商。
- [R 15] 如果切换ECI客户端，对业务的影响须限制在尽可能小。
- [R 16] 在交换**ECI客户端**之后，交换之前应可消费法律要求的**受保护内容**（如加扰PVR内容），无需用户采取任何复杂的行动。

[R 17] **嵌入式CI**不得无理地限制CA/DRM销售商根据市场要求开发不同可互操作/切换**ECI客户端**的可能性。

## 6.6 ECI系统安全相关要求

[R 18] 须可安全且须可按照标准化的方式下载、安装并切换CPE的**ECI客户端**。须采用标准化的解决方案即可下载并安装**ECI客户端**。

[R 19] CPE须提供一个**软件容器 (Software Container)**，后者为任意ECI客户端提供一个统一的抽象层。应注意，统一抽象层为虚拟机提供给ECI客户端之物。

[R 20] **ECI客户端**和**主机**系统须可在任意时刻表明并证明其可信性。

[R 21] **嵌入式CI**须支持**信任主管机构**的开发和确定。

[R 22] **嵌入式CI**不得依赖当前特定的硬件（组件）或特定的操作系统。该要求一般并不禁止高级安全功能，只要这些功能的规范可以公开获取且这些功能与当前相关CPE芯片销售商的安全架构相符。应注意，公开文件中所述的高级安全系统并不视为特定的硬件。

[R 23] **嵌入式CI**系统须允许现有的DVB/ETSI兼容CA/DRM系统向该**嵌入式CI**新系统过渡。应注意，这意味着，运营商可利用其现有的CA/DRM系统访问传统设备及新的、运行与现有CA/DRM系统兼容的ECI客户端的符合ECI标准的设备。

[R 24] **嵌入式CI**须提供钩子（hook），允许向下兼容**嵌入式CI**和ECI实施的未来发展。现有的ECI实施须可处理CPE能力或ECI客户端能力未来的功能扩展所引入的使用权限。

[R 25] **嵌入式CI**须支持包括或不包括智能卡作为安全设备的系统实施，且须为两种解决方案提供资源。

[R 26] **嵌入式CI**须为不同CA/DRM系统应用所需的各种等级的内容安全提供必要的功能。它须适用于大众市场及从低端到高级产品的各种付费产品。

[R 27] 如果切换ECI客户端，**嵌入式CI**不得要求更换任何硬件组件。但是，根据这一要求，切换智能卡或基于智能卡的CA/DRM系统一般不视为更换硬件组件。

[R 28] **嵌入式CI**不得比当前可用的、可比较的嵌入式CA/DRM系统更多地占用CPE的资源（处理能力、内存等）且系统架构的实施不得意味着更高的/额外的成本。

[R 29] **嵌入式CI**须至少支持DVB CSA和AES加扰系统且主机须至少支持MPEG-传输流（ISO/IEC 13818-1 [b- ITU-T H.222.0]）和ISO/BMFF（ISO/IEC 14496-12 [b- ISO/IEC 14496-12:2012]（包括符合ISO/IEC 23001-7 [b- ISO/IEC 23001-7:2011]文件所规定的通用加密方案定义的信令的修正3，但可能采用不同的加密算法）。应注意，支持该要求将与当前DECE所采用的DRM相兼容且将为其他DRM提供**嵌入式CI**支持提供一个标准格式。

- [R 30] 嵌入式CI须提供ECI容器与主机之间接口的适当功能，以支持各种使用权限。
- [R 31] 嵌入式CI须可描述至一个ECI客户端或从一个ECI客户端到另一个ECI客户端的使用权限和使用能力。
- [R 32] 嵌入式CI须在同一设备或不同那个设备上提供ECI客户端之间的安全通信信道。

## 附件A

### <使用案例>

(此附件为本建议书的一部分)

附件A所含使用案例并不涵盖所有情况。

#### A.1 使用案例1

在数字电视业务环境下，需要更换CPE设备中CA/DRM系统可能存在不同的理由。

- 一个数字媒体内容提供商可能决定更换其用户的CA/DRM系统。理由可能是：
  - 不同的技术或商业原因，例如CA/DRM增强功能、安全等级提高或系统性能提升的要求，或者当前系统被深度破解时。
  - 获得了某个网络的新用户，该网络过去从竞争者那里获取业务。
- 平台运营商可能决定变更其平台CPE的CA/DRM系统。理由可能是：
  - 不同的技术或商业原因，例如CA/DRM增强功能、安全等级提高或系统性能提升的要求，或者当前系统被深度破解时。
  - 在购买某个网络后统一不同的技术。
- 某个CA/DRM销售商发展了新客户，该客户运营着一个平台，而其竞争者已经在这个平台上建立了其CA系统；或某个CA/DRM销售商并购了另一个CA/DRM销售商并希望将安全技术进行统一。
- 某个最终用户在任意一家商店购买了CPE并将其连接到接入网提供商的网络中。一个或多个业务提供商在该网络中提供业务。如果最终用户在对应的业务提供商处进行了注册（包括认证和授权），那么他可选择这些业务中的任意一种并下载其CA/DRM系统。过了一段时间，该最终用户决定连接到接入网提供商B的网络。他将其CPE连接到该网络。如果他的CPE支持要求的接收技术（如DVB-C/C2、-S/S2、-T/T2、以太网、xDSL），一个或多个业务提供商可通过该网络提供业务。如果最终用户在对应的业务提供商处进行了注册（包括认证和授权），那么该最终用户可选择这些业务中的任何一种并相应地变更/切换CA/DRM系统。
- 某个CE制造商希望将CPE投放零售市场，该CPE既支持免费电视，也支持付费电视。但是，CPE可能需要在最终用户同意的情况下更新软件，才能改用于收看特定的付费电视业务。

#### A.2 使用案例2

现在，如果要变更在用CA平台已安装CPE的CA系统（无论出于何种原因），总要涉及四方：

- 当前的CA销售商。
- 平台运营商或数字媒体内容提供商。
- CPE制造商。
- 新CA销售商。

当前的CA销售商必须向新的销售商提供技术信息，以访问已安装CPE并获得使用特定硬件组件、协议或这些CPE所采用的软件的许可。总而言之，新的CA销售商需调整期CA系统，以适应在用CPE上已有的功能、硬件/软件限制和协议。CPE制造商需将新的CA系统整合到不同的已安装CPE的软件中。在最差情况下，切换CA/DRM系统甚至可能在技术/商业上无法实现。应改变这种情况，以实现更大的互操作性。

现在，专用安全模块已成为先进CA系统的一部分，绝大多数情况下，CPE是按照专门的CA系统生产的。这可能会限制所切换CA系统可为在用CPE提供的安全等级。应改变这种情况，以便任何安全改进应做到完全的透明。

### A.3 使用案例3

ECI系统须支持仅消费的应用，但也应向二级设备传送**受保护内容**。支持二级设备应用涉及到两种使用案例：

- 集中应用：网关类的、符合ECI标准的CPE向二级设备传送使用权限信息（URI）和加密内容。
- 分散应用：网关类的、符合ECI标准的CPE仅向二级设备传送使用权限信息（URI），二级设备从网络得到加密信息。应注意，ECI系统在二级设备采用DRM客户端方面并没有要求。为了从网关向二级设备传送受保护内容，只需要两个DRM客户端可相互安全通信且内容所有者支持所采用的DRM系统即可。

### A.4 使用案例4（与可信第三方（TTP）有关的使用案例）

现在，任何要求的唯一ID或证书均按排他的方式嵌入在CPE中，由CA/DRM系统的提供商定义。在互操作性方面，这并不是一个适当的解决方案，因为销售商不太可能披露获取唯一ID或证书的机制。例如，“CI plus”联盟已演示过，可向“可信第三方”转让证书的安全处理。可互操作的CA/DRM系统将需要类似的解决方案。

## 参考文献

- [b-ITU-T H.222.0] ITU-T H.222.0建议书 (2006) | ISO/IEC 13818-1 (2007), 信息技术 – 活动图像及相关音频信息的通用编码: 系统。
- [b-ETSI GS ECI 001-3] ETSI GS ECI 001-3, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation.*
- [b-ETSI GS ECI 001-4] ETSI GS ECI 001-4, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine.*
- [b-ETSI GS ECI 001-5] ETSI GS ECI 001-5, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System.*
- [b-ETSI GS ECI 001-6] ETSI GS ECI 001-6, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment.*
- [b-ETSI GS ECI 001-7] ETSI GS ECI 001-7, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Extended Requirements.*
- [b-ETSI ISG ECI] ETSI ISG ECI White Paper-v1\_20 (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions.*
- [b-ISO/IEC 14496-12] ISO/IEC 14496-12:2012, *Information Technology – Coding of Audio-Visual Objects – Part 12: ISO Base Media file format.*
- [b-ISO/IEC 23001-7] ISO/IEC 23001-7:2011, *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files.*



## ITU-T 建议书系列

|            |                                           |
|------------|-------------------------------------------|
| 系列A        | ITU-T工作的组织                                |
| 系列D        | 资费及结算原则和国际电信/ICT的经济和政策问题                  |
| 系列E        | 综合网络运行、电话业务、业务运行和人为因素                     |
| 系列F        | 非话电信业务                                    |
| 系列G        | 传输系统和媒介、数字系统和网络                           |
| 系列H        | 视听及多媒体系统                                  |
| 系列I        | 综合业务数字网                                   |
| <b>系列J</b> | <b>有线网络和电视、声音节目及其他多媒体信号的传输</b>            |
| 系列K        | 干扰的防护                                     |
| 系列L        | 环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护 |
| 系列M        | 电信管理，包括TMN和网络维护                           |
| 系列N        | 维护：国际声音节目和电视传输电路                          |
| 系列O        | 测量设备的技术规范                                 |
| 系列P        | 电话传输质量、电话设施及本地线路网络                        |
| 系列Q        | 交换和信令                                     |
| 系列R        | 电报传输                                      |
| 系列S        | 电报业务终端设备                                  |
| 系列T        | 远程信息处理业务的终端设备                             |
| 系列U        | 电报交换                                      |
| 系列V        | 电话网上的数据通信                                 |
| 系列X        | 数据网、开放系统通信和安全性                            |
| 系列Y        | 全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市           |
| 系列Z        | 用于电信系统的语言和一般软件问题                          |