国 际 电 信 联 盟

ITU-T J.1011

(09/2016)

国际电信联盟
电信标准化部门

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架构、定义和综述

ITU-T J.1011 建议书

国际电信联盟

ITU-T J.1011 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架构、定义和综述

摘要

ITU-T J.1011建议书具体列出用于可交换嵌入式条件接入/数字版权管理（或简称CA/DRM）解决方案的架构，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（CA）系统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.1011	2016-09-02	9	11.1002/1000/12773

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/。

目录

页码

1 范围 1

2 参考文献 1

3 定义 1

3.1 他处定义的术语 1

3.2 本建议书定义的术语 1

4 缩略语和首字母缩写词 2

5 惯例 3

6 可交换CA/DRM嵌入式解决方案的要求 3

6.1 一般说明 3

6.2 ECI系统的技术理念 5

7 信任环境 11

7.1 必要操作流程 12

附录I – 符合ECI的诚信系统的实施 15

参考文献 17

引言

在迅速发展的数字广播和宽带领域，保护由数字接收（CA）和数字版权管理（DRM）实现的服务和内容（包括内容、服务、网络和用户端设备（CPE））至关重要，这样才能保护内容拥有方、网络运营商和付费电视运营商的业务模式。虽然从理念上而言，CA的侧重点是接收服务提供商通过网络分发的受保护内容机制，但DRM的根本是阐明按照签约用户合同而拥有的使用权利的类别和程度。

付费电视运营商已建立了不同数字电视平台，其基本功能采用认可的标准，并辅之以其专有技术。多数用于传统数字广播、网络电视（IPTV）电视或新的过顶（OTT）服务的CA和DRM系统通过将用户端设备（CPE）与其相关专有安全成分相绑定而捕获这些设备。由此，配置用于网络A或平台A的用户端设备无法用于网络B或平台B，反之亦然，这就造成了数字电视消费电子设备市场依然支离破碎，相关规范不仅国与国之间不同，而且平台之间也大相径庭。可拆除的CA/DRM模块仅能部分解决问题：这些模块是CA/DRM系统的专有模块，不仅造价高昂，而且主要用于有线和卫星电视，无法用于诸如平板电脑等现代设备中，因为它们缺乏适当的物理接口。

近期实施的无论是嵌入式的还是可拆除的硬件解决方案都带来了“锁定”效应，极大限制了数字多媒体内容市场上诸多参与方的自由。由于技术进步，使得创新型、基于软件的CA/DRM解决方案得以可行。这些方案在保持极高安全水平的同时实现最大互操作性，因此有望满足市场即将出现的需求，并为新的业务提供方便，同时加大消费者的选择。

消费者能够继续使用其已购买的CPE（如，更换网络提供商，甚或使用不同商用视频门户网站服务的装置）将十分收益。如果在适当安全架构基础上，实现CPE在CA和DRM方面的互操作性，则可达成上述目标。如能确保CA和DRM系统实现消费者友好和内容敏感的互换性，则可避免CPE市场的进一步支离破碎，并促进竞争。

ITU-T J.1011 建议书

可交换CA/DRM解决方案的嵌入式通用接口；
架构、定义和综述

1 范围

本建议书的目的是规定可交换嵌入式通用接口架构的功能实体，以便向CPE下载必要的CA/DRM系统。下载程序在受信任环境中进行，因此，有助于消费通过广播和/或与多种不同类型终端设备实现宽带互连（符合最终用户所获得的内容权利）而提供的受保护内容。本建议书是对整个嵌入式通用接口（ECI）生态系统予以规范的一系列建议书中的一份。

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。所有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。

本建议书引用的文件自成一体时不具备建议书的地位。

[ETSI GS ECI 001-1] ETSI GS ECI 001-1（2014）：用于可转换条件接收/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、定义与综述。

[ETSI GS ECI 001-2] ETSI GS ECI 001-2（2014）：用于可转换条件接收/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 他处定义的术语

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. 高级安全（Advanced Security）：符合CPE的ECI功能，为ECI客户机提供增强型安全功能（硬件和软件）。请注意，细节规范见[b-ETSI GS ECI 001-5]。

3.2.2 ECI（嵌入式CI（Embedded CI））：ETSI ISG“嵌入式CI”中规范的架构和系统，有助于在用户端设备（CPE）中开发和实施基于软件的可交换ECI客户机，因此，在ECI方面实现CPE的互操作性。

3.2.3 ECI客户机（ECI Client）（嵌入式CI客户机（Embedded CI Client））：实施符合嵌入式CI规范的CA/DRM客户机。应注意，CPE中的软件模块以受保护方式提供各种手段来接收和执行消费者在内容分销商和运营商所分销内容方面的特权和权利。这一软件模块还接收消费者使用其权利和特权的条件以及对各种信息和内容进行解密的密钥。

3.2.4 ECI客户机装载器（ECI Client Loader）：ECI主机的一部分软件模块，有助于在ECI主机的ECI容器中下载、验证和安装新的ECI客户软件。

3.2.5 ECI容器（ECI Container）（嵌入式CI Container（Embedded CI Container））：提供一种隔离环境的抽象概念，这一隔离环境包括虚拟机器和一个单一ECI客户机。

3.2.6 ECI主机（ECI Host）：CPE的硬件和软件系统，包含ECI相关功能性并拥有面向ECI客户机的接口。请注意，ECI主机是CPE固件的一部分。ECI主机负责确保将每一个ECI容器加以隔离并提供得到认证的ECI客户机的装载。

3.2.7 ECI主机装载器（ECI Host Loader）：有助于在CPE中下载、验证和安装（新的）ECI主机软件的软件模块。请注意，在多级装载配置中，本术语用以描述装载ECI主机过程中所涉及的所有对安全至关重要的装载功能。

3.2.8 诚信管理机构（Trust Authority (TA)）：负责用于实施ECI的各项规则和细则的组织。请注意，诚信管理机构必须是一个法律实体，只有这样才能够满足合法要求（legal claims）。诚信管理机构必须对可下载CA/DRM生态系统的所有参与方都保持中立。

3.2.9 受信任第三方（Trusted Third Party (TTP)）：在诚信管理机构（TA）管控下，为合规的、ECI系统相关部件制造商发放证书和密钥的技术服务提供商。

4 缩略语和首字母缩写词

本建议书采用下列缩略语和首字母缩写词：

API	应用编程界面
CA	条件接收
CENC	通用加密
CI	通用接口
CPE	用户端设备
DRM	数字版权管理
DVB	数字视频广播
ECI	嵌入式通用接口
HD	高清晰度
HTTP	超级文本传送协议
iDTV	综合数字电视
IP	互联网协议
IPTV	网络电视
LA	许可协议
MPEG	动态图像专家组
OS	操作系统
OSD	屏幕显示
OTT	过顶

PIN 个人识别码
PVR 个人录像机
ROM 只读内存
SI 服务信息
STB 机顶盒
TA 诚信管理机构
TTP 受信任第三方
TV 电视
UI 用户接口
VM 虚拟机器

5 惯例

在本建议书中：

关键词“须”（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，而是指销售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。

在本建议书正文及其附件中，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“须”、“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 可交换嵌入式CA/DRM解决方案的架构

6.1 一般说明

本建议书所涵盖的**ECI**架构、定义和综述是有关通用的、基于软件的、嵌入式和可交换CA/DRM系统架构的、由诸多部分构成的标准的一部分，这一架构将是最为恰当的、可以克服市场支离破碎并促进实现互操作性的、可满足未来需求的解决方案。预计该方式在内容安全方面将带来下列主要益处：

– 由基于软件的实施带来的灵活性和可扩展性
– 可交换性有助于促成实现满足未来需求的解决方案并促进创新
– 适用于通过广播和宽带，包括OTT分发的内容
– 支持多屏幕环境

– 通过避免“锁定”现象，刺激由平台运营商、网络/服务提供商和消费者参与的市场的发展

– 开放生态系统的规范有助于推动市场发展。

ECI系统的目标是在尽可能降低消费者费用并最大程度地减少CA或DRM厂商为付费电视市场开发目标产品的限制条件下，在各相关程度和水平上实现CPE中CA和DRM系统的互换性。ECI的一个核心要素是规范基于软件的CA/DRM客户机与主机系统之间的接口，因此，除其它功能外，ECI还具有下列功能：

– CA针对DRM核的软件容器 – 以下称作ECI客户机，该客户机带有：

  • 与CPE所有相关功能相连的标准化接口

  • 可在其之上运行的标准化虚拟机器（VM）

– 既支持无智能卡系统，也支持智能卡系统的使用

– CPE中包含大量此类软件容器，每一个容器均在其自身的VM实例（instance）上运行

– 安全和标准化的装载理念确保ECI客户机能独立于其它CPE软件得到安装

– 亦称作“芯片组安全性”的高级安全可支持最先进的内容保护

– 方便充分利用由硬件辅助的安全功能

– 用户找到所需进行下载的正确ECI客户机的方法

– 撤销ECI客户机的（一部分）功能和CPE功能

– 适合传统数字广播、IP电视或基于OTT的现代系统。

尽管ECI与已部署的一些解决方案具有相似性，但其实质性差异表现在下列方面：

(1) CA/DRM客户机模块置于软件之内，不再存在于硬件中，因此，如果消费者更换CA或DRM系统，不会产生任何费用。

(2) 可在同一CPE中同时并行实施若干ECI客户机，无需追加成本。

(3) 这些客户机可同时在一个设备中运行。

由此，可以更加轻而易举地互换CA或DRM部分，使最终用户在无需更换昂贵模块的情况下，更换运营商并通过其CPE获得诸多不同运营商的服务。

该完整的多部分标准由一系列规范构成，包括与支撑性规范组合一体的框架规范：

– 第1部分：架构、定义和综述[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容器、装载器、接口、撤销[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：高级安全系统[b- ETSI GS ECI 001-5]

– 第6部分：信任环境[b- ETSI GS ECI 001-6]

– 第7部分：拓展要求[b- ETSI GS ECI 001-7]。

以上部分共同构成一个完整解决方案，方便应最终用户要求，仅通过在任何时候下载ECI客户机即可更换ECI客户机。ECI客户机通过单独装载器安装在CPE的标准软件容器中，并带有单独的安全算法和密钥，以在独立于CPE所有其它软件的情况下，保护ECI客户机的

完整性，并使其免受替换攻击。容器与CPE接口是通用的，并在[b-ETSI GS ECI 001-3]中得到定义，使ECI客户机能够与CPE及其以外的多种不同功能进行互动。

ECI客户机在由[b-ETSI GS ECI 001-4]中定义的虚拟机器实例上运行。

[b- ETSI GS ECI 001-5]规定的高级安全机制旨在保护内容密钥 – 在内容进入到CPE处理器芯片进行内容解密实施时。

本建议书阐述在CPE中实施可互操作CA/DRM系统的架构以及相关接口规范综述。

本ECI规范仅适用于由条件接收和/或数字版权管理系统控制并被服务提供商进行扰码的内容接收和进一步处理。本建议书不包含未由条件接收和/或DRM系统控制的内容。

ECI群规范（Group Specification）的意图是在诚信管理机构掌控下 – [b-ETSI GS ECI 001-6] – 与合同框架（许可协议）、合规性和强健性规则及适当认证程序（见注解）合并使用。请注意，合同框架（许可协议）、合规性和强健性规则及适当认证程序不属于ISG ECI的标准工作范畴。

6.2 ECI系统的技术理念

6.2.1 基本考虑

本建议书结合规范的第2至5和7部分（[ETSI GS ECI 001-2]、[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]、[b-ETSI GS ECI 001-5]和[b-ETSI GS ECI 001-7]），规范有助于在任何时候以独立于在同一主机、多款CPE系统软件或在在其主机上运行的应用的其它ECI客户机下载和安装ECI客户机并对其予以升级、撤销和更换的架构。ECI主机须为两个或在其资源可处理范围内尽可能多的ECI客户机提供运行时间环境。主机中的ECI客户机须并行运行，以便实现源自不同运营商的不同内容流的同时解密或再加密。

本建议书以及[ETSI GS ECI 001-2]、[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]和[b-ETSI GS ECI 001-5]中描述的技术理念既适用于符合DVB多层加密的CA系统，也适用于与DRM系统兼容的通用加密（CENC）系统。

CPE只为具有必要安全功能性的ECI客户机托管专门装载器，以保护ECI客户机的完整性和真实性。该装载器可被随时调用和运行，以便进行下载并在任何时候验证另一个ECI客户机。[b- ETSI GS ECI 001-3]对该装载器及其相关安全设施做出了规范。

具体到该技术理念，每一ECI客户机均在一单独软件容器中得到安装，并带有自身虚拟机器实例（VM实例） – 已由[b-ETSI GS ECI 001-4]予以规范。仅为CA/DRM功能性规定了ECI容器 – [b-ETSI GS ECI 001-3]予以反映。[b-ETSI GS ECI 001-3]详细阐述的与CPE的接口有助于促成各不同CA/DRM功能所需的各种请求和数据交换。这些请求和数据交换可在ECI客户机与主机之间进行，也可在同一主机的两个ECI客户机之间进行，或在不同主机的两个ECI客户机间进行。

以电视为中心的设备被定义为在芯片集中包含MPEG-2传送流处理的设备。ECI要求这些芯片集实施符合ECI的高级安全功能。[b- ETSI GS ECI 001-5]规定了在芯片集中充分利用高级安全机制的内容，以保护与内容相关的密钥（在内容进入到CPE处理器芯片的内容解密设施过程中）。该高级安全理念有助于使用这一设施的所有ECI客户机在必要时同时并相互间独立运行。

其它环境中的设备，特别是IP电视和平板电脑、智能电话等，通常在软件中实施更多功能性，并提供双向IP通信，且有助于实现有针对性的新型安全增强机制。由于这些装置使用的芯片集包含多种不同处理安全功能软件，因此，ECI要求实施专门的、硬件辅助安全和强健性功能，以实现ECI合规性。因此，[b- ETSI GS ECI 001-3]这一规范包含ECI客户机获得主机技术能力和功能性相关参数的方法，并在尽可能适用情况下，包括对高级安全的可能支持（如[b- ETSI GS ECI 001-5]所规范）。

高级安全功能同时为在CPE中活动的任何ECI客户机提供。ECI客户机还可在带有符合DVB的CA系统或带有CENC的DRM系统（以同时加密或多加密模式运行）的平台中得到部署，前提是这些系统的服务器一侧符合相应的DVB/CENC后台标准。

6.2.2 架构综述

ECI有助于CA/DRM提供商在个人用户范畴内实施条件接收（CA）及数字版权管理（DRM）解决方案。图1所示为完整ECI实施充分支持的参考配置。

为了在个人消费者范畴内支持多屏幕环境，该范畴内的ECI客户机可相互通信，并可利用与提供商之间的双向网络，这取决于所提供的适当网络以及CA/DRM系统及其ECI客户机的支撑功能性。[b-ETSI GS ECI 001-3]做出了进一步详细规范。

可以如此实施ECI客户机，即，使其成为不符合ECI的客户机的网关，因此，[b- ETSI GS ECI 001-5]规定了必要的挂钩（hooks）。专有客户机的具体协议和实施不属于ECI规范的范畴。

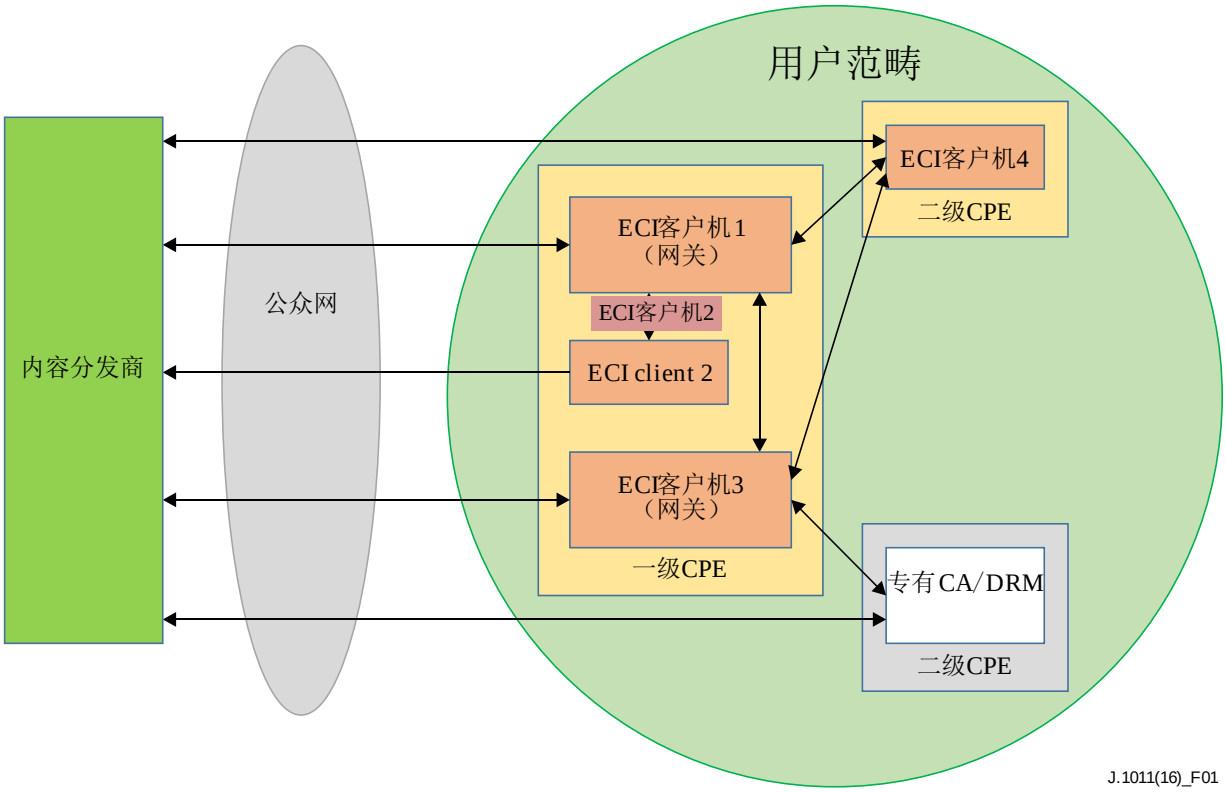


图1 – 单一客户范畴内的ECI客户机

ECI规范除定义其它内容外还定义了ECI容器与ECI主机之间的接口。图2所示为一个带有ECI容器以及ECI容器与之或可能与之进行通信的、ECI主机中其它功能的CPE框图。其中一些功能为可选功能。在安装ECI客户机和启动ECI客户机过程中，主机具体规定它向ECI客户机提供哪些相关功能。

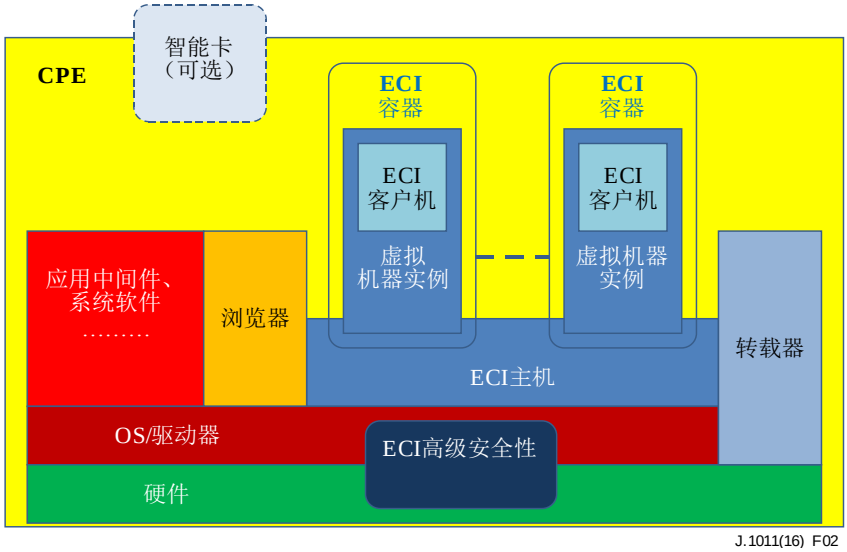


图2 – 带有嵌入式ECI客户机且每一客户机均有其自身ECI容器和虚拟机器实例的CPE框图

首先，该理念以分层装载器概念（参见图3）为基础，后者包括基于芯片的装载器、系统软件装载器和ECI客户机装载器。

ECI主机装载器进行ECI主机软件装载，除其它元素外，其中包含虚拟机器、获取高级安全构件以及ECI客户机装载器。一个ECI主机可以将多个ECI客户机装载到单独虚拟机器实例中，而且这些实例各自独立运行。

将ECI客户机装载到系统中时即在创建虚拟机器实例（ECI客户机装载至此）。该VM实例是ECI客户机与主机之间的一个沙盒（sandbox）。ECI客户机与VM实例之间的接口是群规范（GS）装载规范的一个重要接口。该接口还规定了这种ECI客户机多个实例之间的信息流/协议以及到CPE内部其它功能的信息流和协议，如高级安全性、显示等等。请注意，其它ECI客户机不一定需要处在同一ECI主机中。[b- ETSI GS ECI 001-3]规定了该接口与通信协议的规范。

ECI主机本身则有赖于制造商的实施。

该主机与OS和驱动器层连接并提供ECI客户机接口规范确定的所有功能。ECI并未规定ECI主机，但需得到TA的认证，以确保符合ECI客户机接口规范。

6.2.3 符合ECI的设备的必备功能

ECI涉及繁复多样的使用情形（见图1），因此，ECI必须处理包括iDTV、STB、个人录像机（PVR）、IP电视、平板电脑、智能电话在内的一系列装置。尽管ECI提供统一安全框架，但这些装置的能力大相径庭。ECI将以电视为中心的装置与以其它环境为中心的装置加以区分，后者包括但不限于IP电视和平板电脑。

以电视为中心的装置被定义为在芯片集中包含MPEG-2传送流处理的装置。ECI要求这些芯片集实施符合ECI的高级安全功能。以电视为中心的、符合ECI的CPE须符合[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]和[b-ETSI GS ECI 001-5]中定义的功能。

用于其它环境的装置，特别是IP电视、计算机和平板电脑，通常在软件中实施更多功能性并与双向IP通信相连。这有助于实现不同类型安全机制。这些装置中所用的芯片集包括多种不同安全处理功能硬件，且ECI要求在芯片集中实施专门的、由硬件协助的安全和强健性功能。[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]和[b-ETSI GS ECI 001-5]具体规定了充分利用这些功能性的机制。

6.2.4 ECI主机与ECI客户机之间的必要接口

ECI容器是一个技术概念，将VM和ECI客户机相结合，目的是将VM和ECI客户机与其余CPE相隔离并对其加以屏蔽。虚拟机器是ECI主机的一种功能。ECI通过装载ECI客户机创建虚拟机器实例。虚拟机器提供与ECI客户机连接的必要接口并将其与ECI主机相连接。有关ECI的规范确定了VM与ECI客户机之间的接口，有关符合ECI的装置的高层架构，亦请见图2。该接口提供某些应用程序接口（API），同时也建立了安全通信信道。

以下重点列出一些重要软件接口：

– 由ECI主机向ECI客户机（反之亦然）提供能力信息的接口
– 通向CPE输入和输出信号处理的接口
– 通向高级安全硬件/驱动器群的接口
– 通向装载器功能的接口
– 通向支持用户互动的接口

– 通向加密和解密功能的接口
– 通向可选智能卡读卡器的接口
– 通向具体安全功能（如指纹和水印）的接口
– 通向本地存储的接口。

ECI客户机的所有接口均通过虚拟机器这一手段加以提供。

除便于进行安全通信的接口外，还存在一些通信协议，特别是正在规范旨在建立无论是内部还是外部的ECI客户机之间通信的协议。

可以单向或双向方式将CPE与任何类型网络连接并可同时与若干网络连接。该设备无需永远与任一特定网络连接（下载/存储内容）。

6.2.5 最小用户接口和显示功能

为与用户进行通信，须为ECI容器提供最小用户接口（UI）和屏幕显示（OSD）设施，这已在[b- ETSI GS ECI 001-3]中得到规范。该功能用来向用户显示已生成或利用CA/DRM系统发送的信息。此外，还利用该功能方便用户进行输入，如输入个人识别码（PIN）。[b-ETSI GS ECI 001-3]对此予以了详细规范。

用户通过ECI客户机在本地与CA/DRM系统互动。

6.2.6 虚拟机器

ECI客户机在一标准化虚拟机器（VM）上运行，后者在[b-ETSI GS ECI 001-4]中得到规范。每一安装的ECI客户机均须拥有自身的VM实例。VM实例为执行条件接收核或数字版权管理客户机应用提供安全环境。VM还提供API，可通过这些以标准化方法获取ECI主机环境中的资源。

6.2.7 高级安全设施

ECI确定建立安全内容保护系统所需的最低必要安全功能性。ECI要求在硬件元素基础上进行增强。在以电视为中心的设备中，这一功能性通过具体针对电视的专用高级安全功能实现。该功能在芯片系统（SoC）中规定了通常称之为“关键阶梯块”（Key Ladder Block）这一具体能力。高级安全设施的一项基本任务是在将内容保护密钥由ECI客户机传向CPE的内容解密设施或将受保护内容从一个ECI客户机传向另一个ECI客户机时对这些密钥加以保护（见图1）。[b-ETSI GS ECI 001-5]规定的高级安全系统支持不同的同时控制字（Control Word）流和同时要求其服务的不同ECI客户机。此外，高级安全设施在为主机和ECI客户机核实软件下载方面发挥着关键作用。

其它环境使用的设备，特别是IP电视、计算机和平板电脑通常在软件中实施更多功能性并与双向IP通信相连接。ECI规定的高级安全理念和机制相同，但在[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]和[b-ETSI GS ECI 001-5]这些设备安全架构中，其图形显示不同。

CPE是否提供高级安全会在ECI客户机安装和启动过程中对其进行通报。

6.2.8 再扰码

由符合ECI的CPE接收的受保护内容可能不会立刻得到消费。符合ECI的设备提供下列功能：

– 本地存储：
  - 由CPE控制
  - 由CA或DRM客户机控制
– 网关：
  - 在DRM客户机控制下为外部装置提供受保护内容要素
  - 为在同一CPE内或在另一个符合ECI的CPE中运行的另一个ECI客户机提供受保护内容要素。

为支持这些功能，符合ECI的设备有能力对内容重新扰码。ECI系统并不规定传送机制，也不规定可用的受保护内容存储和向其它设备进行提供的DRM功能性。在[b-ETSI GS ECI 001-5]中，ECI主机与ECI客户机之间必要的接口得到定义。

6.2.9 ECI装载器功能

符合ECI的CPE须提供装载器功能，以方便装载和安装ECI系统相关软件模块并保护这些模块的完整性，同时使其免于被替代。

最初，与芯片集成一体的装载器进行系统软件装载器的装载。这一嵌入式装载器旨在确保只有经认证的系统软件装载器才可得到安装和启动。系统软件装载器包括ECI主机装载器，因此，系统软件装载器需由诚信管理机构签署。系统软件装载器可包括其它系统软件装载器，后者与ECI功能无关，且与系统的安全相关要素也无关联。ECI主机软件包括ECI客户机装载器，后者可应要求装载ECI客户机。

ECI客户机在其自身ECI容器中进行安装和启动过程中，由ECI主机告之其所拥有的设施，如记录设施、HD设施、智能卡识读器、指纹和水印设施、网络以及是否符合框架规范（本建议书）和[b-ETSI GS ECI 001-3]、[b-ETSI GS ECI 001-4]和[b-ETSI GS ECI 001-5]及 [b-ETSI GS ECI 001-6]。

[b-ETSI GS ECI 001-3]规定了带有相关安全设施的ECI装载器。

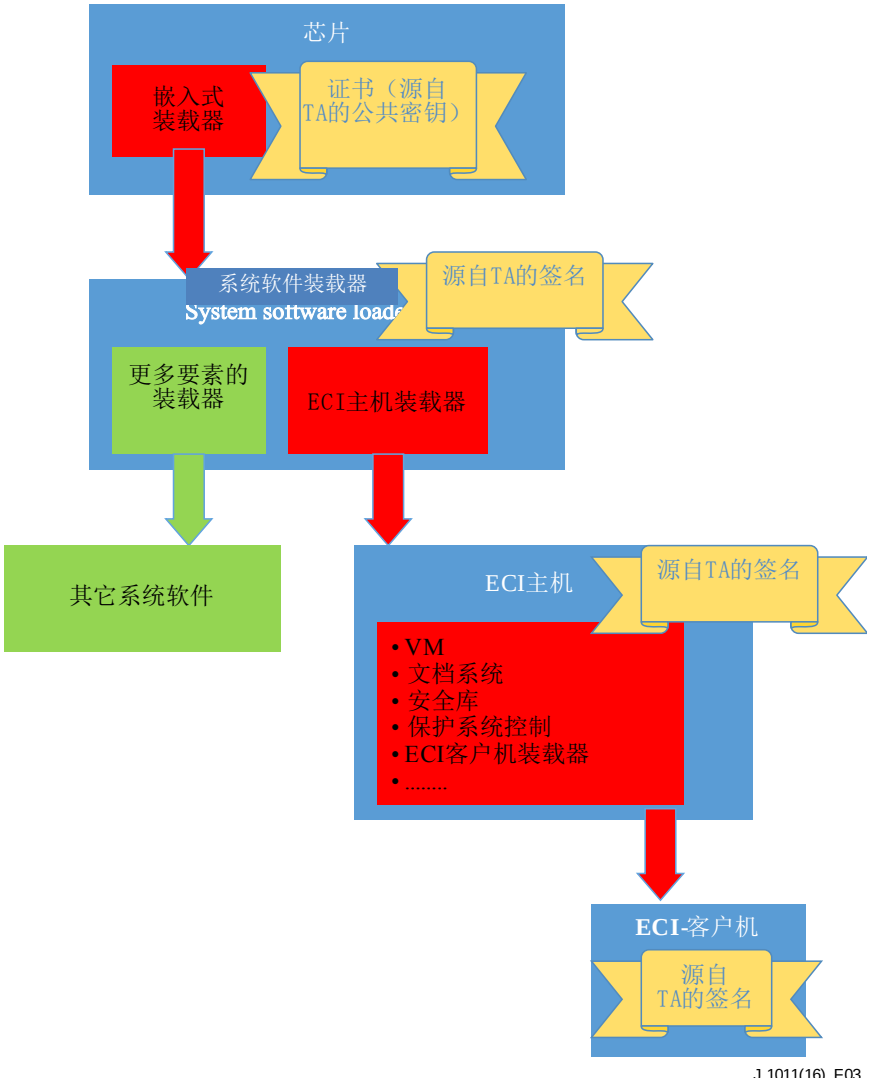


图3 – 装载器分层概念

6.2.10 撤销

诚信管理机构可决定将某一制造商生产的某一CPE、其一系列CPE、一类CPE或所有CPE列入黑名单。内容提供商和运营商可以从其服务经销点取消这些所涉CPE。所用方法便于其它运营商和内容分销商按照意愿继续为这些CPE提供服务。

撤销可以阻止运营商或内容提供商向所涉CPE提供一些服务或所有服务。这属于相关CA或DRM系统的功能问题，不属于本建议书的范围。

[b-ETSI GS ECI 001-3]对撤销程序做出规定。

7 信任环境

为了能够建立基于嵌入式CI的系统，必须创建一种信任环境。有关信任环境的细节亦超出ECI规范的范围，[b-ETSI GS ECI 001-6]规定的原则对于充分了解ECI的工作方法至关重要。

诚信管理机构（TA）是管理适用于ECI架构实施的所有规则和细则的组织。诚信管理机构必须是一个法律实体才能够实现法律要求。

诚信管理机构需要对可下载CA/DRM生态系统中的各方保持中立，这些包括：

– CPE制造商
– CA/DRM（ECI客户机）制造商
– 芯片集制造商，其构件包括不可更换的安全处理器密钥和证书，后者对于实现主机和合规的CA/DRM系统之间的互动必不可少
– 平台运营商：平台运营商控制着CA/DRM系统的所有必要元素，例如，平台运营商是服务提供商或网络运营商
– 必要时还包应用提供商。

受信任第三方（TTP）是一技术服务提供商，负责为ECI系统相关部分的合规制造商发放证书和密钥。TA持有信任根（root），因此，对密钥和证书予以保证。

诚信管理机构和受信任第三方共同构成诚信链的基础，因此，必须参与整个进程- 生产（芯片和CPE）、运行（安全的ECI客户机下载和激活）及控制措施（如取消）。

诚信管理机构作为法律实体通过称作许可协议的合同框架确保诚信环境的运行，在该环境下所涉各方各司其职并承担各自的责任。诚信管理机构/受信任第三方按照许可协议生成并发放密钥对、证书、测试资格证书和运营商ID等。

一家TA负责建立所有市场参与方之间的诚信，不能有第二家TA为同一环境“第二次”建立诚信，然而，在一国或一个区域或某些市场部分及生态系统内可存在多个TA。

如果同时有多个TA并存，则TA A与TA B之间的相互信任是一个前提条件，只有这样，在TA A那里注册的设备才可以在TA B管辖的域内使用。

7.1 必要操作流程

本节首先概述可满足市场不同参与方需求的必要操作流程，以便实施基于**ECI**技术的业务。此外，所述流程的基础是实施**ECI**系统必不可少的基本要素。图4所示为这些技术成分与相关市场参与方之间的互动。

备注：这一描述是一般性描述，并非旨在反映任何现有的专有解决方案或任何目前正在进行的标准化活动。

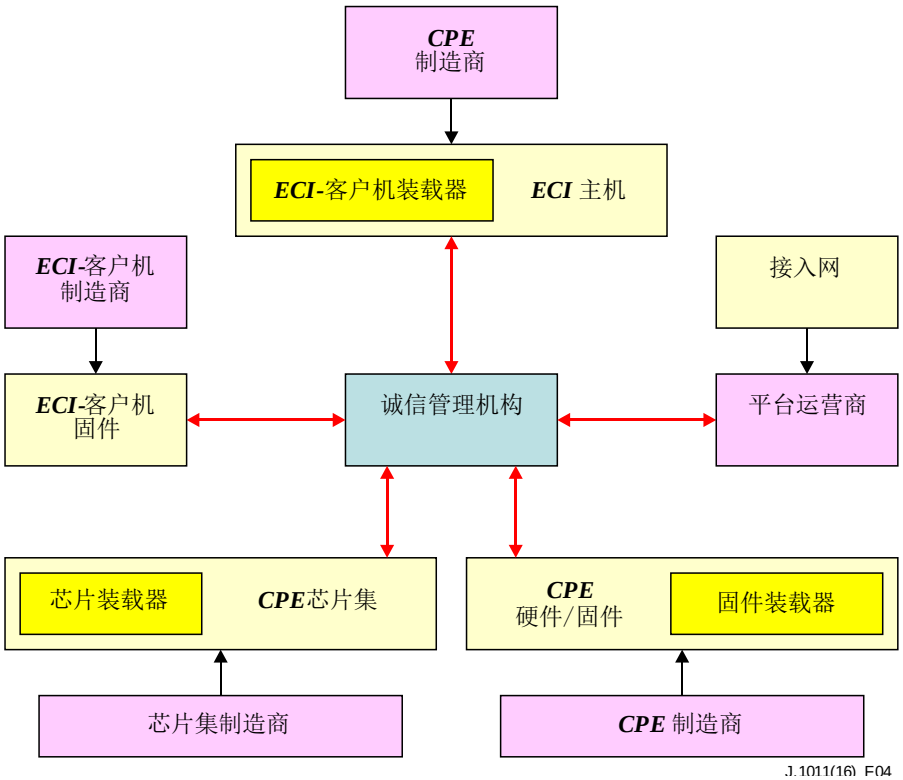


图4 – 诚信管理机构（TA）与相关市场参与方之间的必要诚信管理

诚信环境的操作和相关合同问题（见图4中的红色箭头）如下：

1) 完整性

完整性意味着一个市场参与方能够核实由另一个市场参与方提供的硬件/软件部分不被任何未经授权的方面修改，而且满足相关规范和强健性规则的要求。根据诚信管理机构/受信任第三方发放的测试资格证书，可通过合适的证书、签名和测试程序满足上述要求。

2) 真实性

真实性意味着源自诚信管理机构（TA）合同方并已通过必要的核实和认证程序的硬件/软件成分能明确无误地与所涉合同方相联系，因此，可以从任何被克隆的成分中区别开来。任何ECI系统都可以证明相关硬件/软件成分的真实性。

3) 合同框架

由作为法律实体的诚信管理机构确立的合同框架须包含合规性和强健性制度和认证程序，以便为建立ECI系统提供必要环境。

4) 补救措施

如果ECI系统的任何硬件/软件成分不再合规，则诚信管理机构为该部件提供方确立相关程序，以便在合理时间范围内恢复生态系统的完整性。

基本技术成分（图4中的黄色框）为：

1) CPE芯片集

CPE芯片集是CPE硬件中的主要成分，“通常包括芯片系统（SoC）”，因为平台运营商和内容提供商具有现实需求，此外，通常在CPE芯片中包含芯片装载器。

2) CPE硬件

确保CPE芯片集得到安全实施、避免出现对存储部分的未经授权访问（闪存、内存）并保护接口都是至关重要的问题。

3) 不同装载器

芯片装载器下载不同更多装载器，这取决于CPE硬件/软件的配置。

4) CPE固件

CPE固件与ECI客户机和CPE所有相关硬件接口都有多层互动。安全性由详细的规范和适当的合规性及强健性规则加以保证。

5) ECI客户机

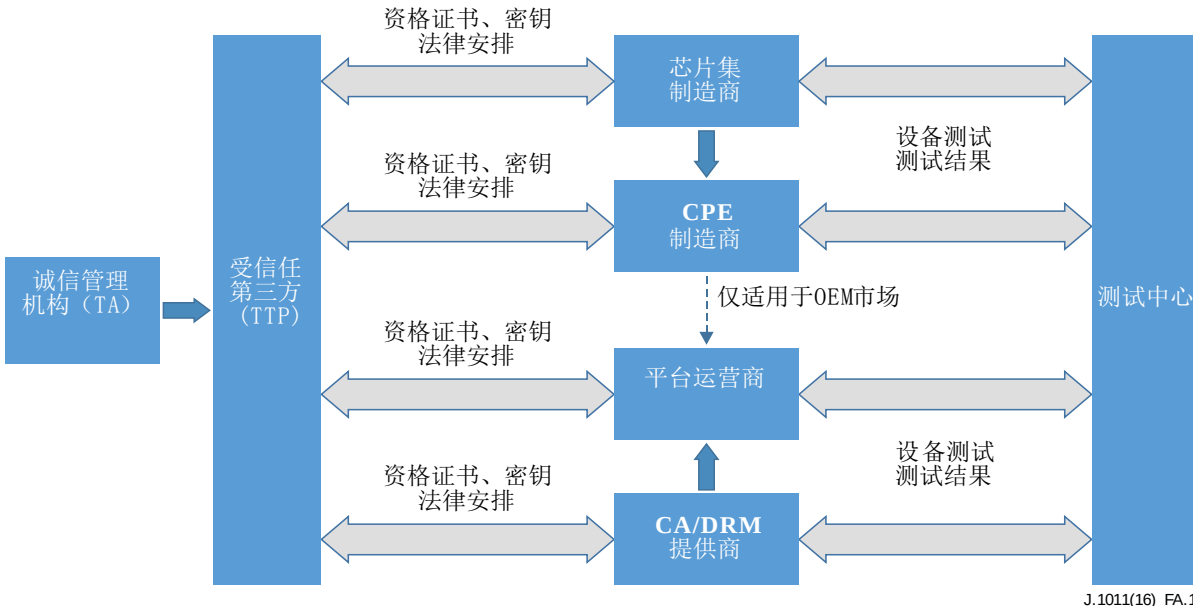
ECI客户机提取由CPE前端提供的所有CA和DRM相关信息，并启动CPE装置中的相应设置（去扰码、接口），且显而易见需要与CPE固件进行密切和安全互动。

附录I

符合ECI的诚信系统的实施

（本附录不构成本建议书不可分割的部分）

附录I首先概述可满足市场不同参与方需求的必要操作流程，以便实施基于ECI技术的业务。图I.1显示了总体工作流程概况。此外，所述流程的基础是实施ECI系统必不可少的基本要素。第7.1节中图4所示为技术成分与相关市场参与方之间的互动。



注 – 受信任第三方（TTP）和测试中心是诚信管理机构（TA）在进行认证和密钥发放过程中的合同伙伴

图I.1 – 总体工作流程概况

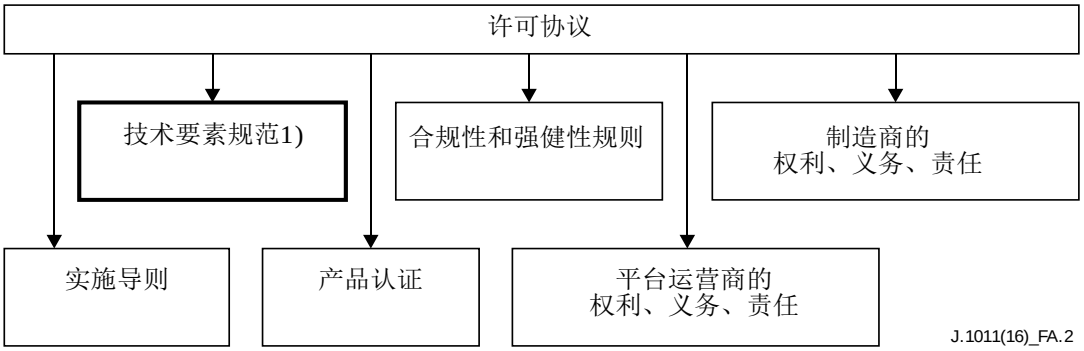
法律/合同框架

安全的诚信管理只能在得到明确无误确定的法律和合同框架内进行，其中许可协议（LA）是该框架的核心内容。TA为任何寻求实施规范的方面提供许可协议，无论它们是CPE制造商、CA/DRM系统厂商、芯片制造商还是其它技术提供商、平台运营商等。

有鉴于此，许可协议对于TA而言是一种最基本的法律手段，用以为横向市场创建、维护和提供安全的、但又是用户友好的方法，以便后者接收和获得将CPE与符合相关使用规则的选定提供商连接时所需的所有操作工作要求的必要以及其它安全相关材料和信息。同样，许可协议框架有助于TA在消费者被提供商中断时以在技术和经济上尽可能可行的方式处理有关撤销所有安全资料的问题。

许可协议还有助于协调和统一一致地应用合同框架的其它要素，如技术规范、合规性和强健性规则、义务与责任、测试与认证、实施导则等。

图I.2显示了许可协议的构成内容。



图I.2 – 许可协议的构成内容

这些规范将在ETSI ISG ECI中作为群规范加以确定。

参考文献

[b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006)/ISO/IEC 13818-1:2007, *Information technology -- Generic coding of moving pictures and associated audio information: Systems*.

[b-CENELEC EN 50221] CENELEC EN 50221 (1997), *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications*.

[b-CI Plus Specification] CI Plus Specification (V1.3.1) (2011), *Content Security Extensions to the Common Interface*.

[b-ETSI EN 300 468] ETSI EN 300 468 (V1.13.1) (2012), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*.

[b-ETSI ISG ECI] ETSI ISG ECI White Paper (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*

www.etsi.org/deliver/etsi.../ECI/.../gs_ECI00101v010101p.pdf

[b-ETSI TS 101 699] ETSI TS 101 699 (V1.1.1) (1999-11),*Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*".

http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+101+699-v1.1.1-1999-11

[b-ETSI TS 103 162] ETSI TS 103 162 (V1.1.1) (2010), *Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification*.

[b-ETSI TS 103 205] ETSI TS 103 205 V1.1.1 (2014), *Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification*

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
系列J	**有线网络和电视、声音节目及其他多媒体信号的传输**
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

瑞士印刷
2018年，日内瓦