国 际 电 信 联 盟

ITU-T J.1015.1

（04/2020）

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

用于可转换式CA/DRM解决方案的嵌入式通用接口；高级安全系统 – 密钥阶梯数据块：验证控制词-用法规则信息与相关联数据1的认证

ITU-T J.1015.1 建议书

国际电信联盟

ITU-T J.1015.1 建议书

用于可转换式CA/DRM解决方案的嵌入式通用接口；高级安全系统 – 密钥阶梯数据块：验证控制词-用法规则信息与相关联数据1的认证

摘要

ITU-T J.1015.1建议书是多份成果文件的一部分，涉及用于可转换式有条件接入/数字版权（CA/DRM）解决方案规范的嵌入式通用接口的高级安全系统密钥阶梯数据块。

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.1015.1	2020-04-23	9	11.1002/1000/13837

关键词

有条件接入、CA、数字版权管理、DRM、交换

* 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

引言

本建议书[1]旨在促进电子通信服务，特别是广播和视听设备市场的互操作性和竞争。然而，根据成员国的具体情况，同时亦存在可用、适当和有益的其他技术。

为了保护内容免受未授权访问，内容提供商对它们的数字内容进行了加密，并采用了一种**内容保护系统**[2]。用户使用**内容接收器**来访问受保护的内容。因此，**内容接收器**包含一个可以实施一次或多次内容解密操作的芯片组。采用密钥建立协议来保障内容解密密钥从**内容保护系统**到芯片组的传输安全。在本文中，芯片组内实施的协议步骤被称为“密钥阶梯”。

密钥阶梯和该协议亦可用于保障从内容加密密钥到芯片组的传输安全。在芯片组对内容进行再加密的情况下，需要使用这类密钥。为此，芯片组可能会实施一次或多次内容加密操作。个人视频录制受保护内容，并将受保护内容传输至另一个不同的**内容保护系统**是典型的内容再加密使用案例。在本文中，内容解密密钥和内容加密密钥皆称为“**控制字**”（**CW**）。

本建议书亦介绍了一种认证机制。这种机制与密钥阶梯密切相关，且可能用于实体认证；换言之，这种机制可能用于认证芯片组。

本建议书中介绍的密钥阶梯和认证机制对**内容保护系统**和**内容提供商**皆无限制。因此，**内容提供商**可以使用任何合规的**内容保护系统**，用户可以使用**内容接收器**访问采用合规**内容保护系统**的任一**内容提供商**的内容。

认证机构负责管理建议书介绍的机制中各个芯片组的公钥认证。尤其是，**认证机构**负责向希望采用密钥阶梯和/或认证机制的**内容提供商**发放此类证书和证书吊销信息。然后，内容提供商将该证书和证书吊销信息作为输入信息用于他们合规的**内容保护系统**；如[ITU-T J.1015]第7条所述，芯片组证书包含的公钥信息使**内容保护系统**能够产生与该芯片组的密钥阶梯和认证机制适配的输入信息。

---

1 附录一确定了几个需要进一步发展的领域。

2 本建议书案文的黑体字表示用门用于嵌入式通用接口背景的术语，这些术语可能不同于通用术语。

ITU-T J.1015.1 建议书

用于可转换式CA/DRM解决方案的嵌入式通用接口；
高级安全系统 – 密钥阶梯数据块：
验证控制词-用法规则信息与相关联数据1的认证

1 范围

本建议书介绍了用于**内容接收器**芯片组的一种密钥阶梯数据块。该密钥阶梯数据块由一个保障**控制字（CW）**安全传输至芯片组的密钥阶梯和一个认证机制组成。本建议书亦具体介绍了与合规芯片组个性化相关的问题。

本建议书旨在供芯片组制造商使用。

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。所有建议书和其他参考文献均会得到修订，因此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建议书清单定期发布。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T J.1015] ITU-T J.1015（2020）建议书，用于可转换式CA/DRM解决方案的嵌入式通用接口；高级安全系统 – 密钥阶梯数据块

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 认证机构:嵌入式公共接口（**ECI）生态系统**中负责管理公钥证书的一方。系统中的所有其他方都信任证书颁发机构负责执行与证书相关联的操作。

3.2.2 芯片组ID：用于识别（**ECI）生态系统中**芯片组的非机密数字。

3.2.3 内容保护系统：ECI生态系统中的系统，采用加密技术管理对内容和服务的访问。该术语可能常会与另一个“服务保护系统”交替使用。这类典型系统例如，有条件访问（CA）系统或数字版权管理（DRM）系统。

3.2.4 内容提供方：向**ECI生态系统**中的**内容接收设备**分发数字内容的一方。

3.2.5 内容接收设备：用于在**ECI生态系统**中访问数字内容的设备。内容接收设备包含配备**内容解扰器**的芯片组。

3.2.6 内容解扰器：ECI生态系统芯片组中能够解密内容的组件。内容解扰器亦能为内容加密（旨在实施内容再加密）。在本建议书中，内容加密/解密使用**对称加密方案**。对于MPEG-2内容，内容加密和解密也分别称为加扰和解扰。

3.2.7 控制字：用于加密和解密**ECI生态系统**中内容的密钥。在数字版权管理系统中，控制字通常被称为内容密钥。

3.2.8 加密散列函数：ECI生态系统中的非加密函数，可接受任意大小的数据（称为消息）作为输入，并产生固定大小的输出数据块（称为消息摘要）。本建议书中**加密散列函数**的假定属性是**加密散列函数**表现为随机函数，并且具有第二原像抗性。

3.2.9 数字签名方案：键控非对称加密方案，用于保护**ECI生态系统**中数据的真实性。**数字签名方案**由密钥生成算法、签名生成操作和签名验证操作组成。密钥以（秘密/专用密钥、公钥）对的形式生成。使用秘密/专用密钥进行数据签名，并使用相应的公钥验证签名。本建议中指定的**数字签名方案**用于确保[b-ROEL]中定义的消息的真实性；特别要指出，在本建议书中，该方案不用于提供不可否认性或源认证。

3.2.10 ECI生态系统：由一个托管机构和若干平台以及**ECI**（符合客户驻地设备的要求）组成的商业运营系统。

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：

AD1 关联数据1

AK 认证密钥

CA 有条件访问

CW 控制字

DRM 数字版权管理

ECI 嵌入式通用接口

ID 身份

LK 链路密钥

SHA 安全散列算法

SPK 发送方公钥

SSK 发送方秘密密钥/私钥

T 标签

URI 使用规则信息

5 惯例

本建议书案文的黑体字表示用门用于嵌入式通用接口背景的术语，这些术语可能不同于通用术语。

6 控制字的认证-使用规则信息和关联数据1

关于[ITU-T J.1015]第7条中的规范细节，规定了密钥阶梯数据块的几项输入，其中包括：CW-URI、AD1、τ_b、SPK-URI、SPKi、加密LK以及签名芯片组标识。这些输入的认证依赖于隐式认证；如果为任何密钥阶梯输入提供了不可信的值，则计算将得出无效的连续值，且内容不能成功解扰。

考虑到输入信息的特性，发送方很可能不采用任何加密方案来发送SPK_i、SPK-URI和τ_b。尤其是，τ_b可利用关联数据验证例程进行验证，因此无需采用明确的认证方案。

如果服务提供商需要，他们可以为密钥阶梯数据块的CW-URI和AD1输入引入其它明确的认证方法。这种功能可以方便用户以及服务提供商的运营优势。

本建议书介绍了一种在CW-URI和AD1是密钥阶梯数据块的输入信息的情况下，对CW-URI和AD1应用认证方案的办法。此方法可通过采用数字签名方案实现，该方案已采用SSK在芯片组ID || E（SPK, LK） 上得到应用。服务运营商可选择认证CW-URI或AD1，或者同时认证二者。

若服务运营商希望保护CW-URI 和/或 AD1，那么需要使用本附件中介绍的方案。

见图1。

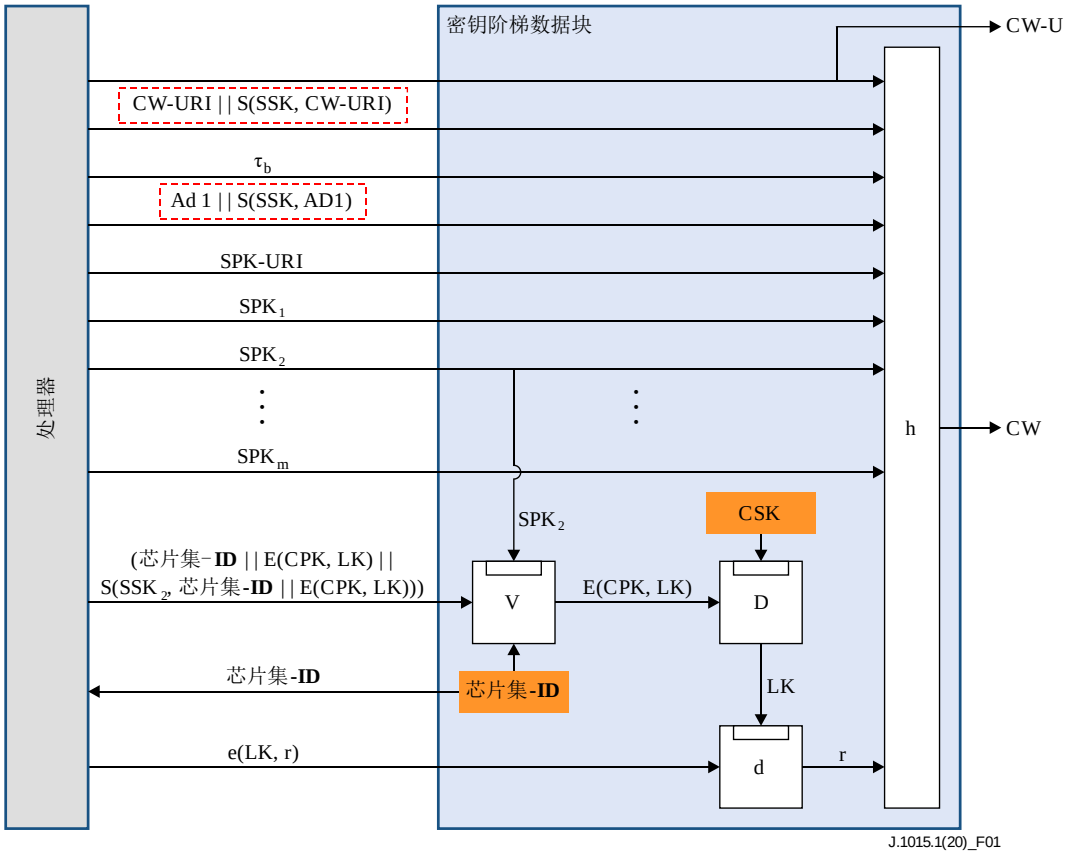

图1 – 控制字的认证-使用规则信息和关联数据1

6.1 控制字的认证-使用规则信息

计算CW-URI ||签名（发送方）

1) 采用SSK_i为比特串CW-URI签名；签名用S（SSK_i、CW-URI）表示。

2) 将该签名附加在比特串CW-URI之后。

检索CW-URI（密钥阶梯数据块）

1) 检查输入数据的长度。若CW-URI长度为64位，那么，密钥阶梯数据块应执行[ITU-T J.1015]第7.3.1条中介绍的正常流程，并中止CW-URI的认证流程。否则，若其长度多于64位，则执行CW-URI认证流程并进入下一步。

2) 检查SPK-URI和[ITU-T J.1015]第7.3.2条中规定的使用规则是否允许V使用SPK_i验证签名。如果不允许，则密钥阶梯数据块将中止计算。

3) 使用收到的（CW-URI | |签名）和SPK_i验证签名。如果签名无效，则密钥阶梯数据块将中止计算。

4) 检索CW-URI。

6.2 认证关联数据1

计算AD1 ||签名（发送方）

1) 采用SSK_i为比特串AD1签名；签名用S（SSK_i, AD1）表示。

2) 将该签名附加在比特串AD1之后。

检索关联数据1（密钥阶梯数据块）

1) 检查输入数据的长度。若AD1长度为256位，那么，密钥阶梯数据块应执行[ITU-T J.1015]第7.3.1条中介绍的正常流程，并中止AD1的认证流程。否则，若其长度多于256位，则执行AD1认证流程并进入下一步。

2) 检查SPK-URI和[ITU-T J.1015]第7.3.2条中规定的使用规则是否允许V使用SPK_i验证签名。若不允许，那么密钥阶梯数据块应中止计算。

3) 利用收到的（AD1||签名） 和SPK_i验证签名。若签名无效，那么密钥阶梯数据块应中止计算。

4) 检索AD1。

附录I

有待进一步发展的领域

（本附录不构成本建议书不可分割的部分）

现已确定，本建议书需要进一步完善和验证，以满足[b-ITU-T J.1010]规定的要求，并且[b-ITU-T J.1010]需要更新，以反映MovieLabs增强内容保护（ECP）规范[b-ECP]的要求。 [b-ITU-T J.1011]、[b-ITU-T J.1012]、[b-ITU-T J.1013]、[b-ITU-T J.1014]、[ITU T J.1015]和ITU-T J.1015.1建议书今后应更新，以体现[b-ITU-T J.1010]的更新。

国际电联的许多成员国，以及来自世界各地不同行业的利益攸关方，包括设备和电子组件制造商、版权内容的所有者和许可持有方、过顶（OTT）和线性电视服务提供商以及有条件接入系统（CAS）和数字根管理（DRM）解决方案提供商，都表示担心嵌入式通用接口（ECI）不能完全满足ECP的要求，也不能满足更广泛的行业内容保护要求。

更具体而言，相关方在向ITU-T第9研究组会议（2020年4月16日至23日）提交的文稿中提出了他们的关切。以色列、澳大利亚、ITU-T部门成员三星公司、SG9联合天空集团和MovieLabs建议在ECI建议书中纳入一些修改，但相关方未就此达成一致。这些项目在[b-SG9报告17 附件1]中进行了盘点。

他们的建议旨在：

1) 缩小范围，简化ECI系统；
2) 移除DRM
3) 取消内容的再加密；
4) 取消软件管理；
5) 添加用于安全存储和加密操作的API；
6) 允许使用针对特定供应商的密钥阶梯；
7) 采用ITU-T J.1207 TEE的要求；
8) 为VM纳入TEE实现；
9) 升级密码算法的强度，例如，使用SHA-384；
10) 使用标准证书，如ITU-T x . 509；
11) 重新考虑客户机之间的沟通；
12) 与ETSI进行更多联络；
13) 执行额外的同行评审；
14) 探索托管机构模式的替代方案；
15) 进一步定义ECI合规性和稳健性规则的技术方面；
16) 增加对多样性的要求，例如地址空间随机化；
17) 增加运行时间完整性检查的要求。

这些建议反映出内容保护及其破坏威胁在不断演变。ECI的设想是在ITU-T 建议书获得批准前十年出现的。像ECI这样的系统需要根据当前的攻击技术和行业保护要求定期评估。

当前存在实现互操作性的其他机制。特别是对于数字版权管理的使用案例，大多数互联网视频服务已经部署了其他解决方案来提供互操作性并满足他们的需求。

鉴于许多成员国将国际电联的标准视为其市场和行业发展的有影响力的指导来源，因此做出进一步澄清至关重要。问题清单确保ECI在国内市场的实施能够充分理解ITU-T 建议书的含义，并确保在思考要求消费者数字电视设备具有互操作性的立法、法规或市场需求时，能够考虑到这些问题。本建议书还可确保技术设备制造商在为不同市场开发产品时能够考虑到这些问题，这些制造商可能更喜欢使用一套独特的要求或其他标准来设计产品。

参考文献

[b-ITU-T J.1010] Recommendation ITU-T J.1010 （2016）, *Embedded common interface for exchangeable CA/DRM solutions; Use cases and requirements.*

[b-ITU-T J.1011] Recommendation ITU-T J.1011 （2016）, *Embedded common interface for exchangeable CA/DRM solutions; Architecture, definitions and overview.*

[b-ITU-T J.1012] Recommendation ITU-T J.1012 （2020）, *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation.*

[b-ITU-T J.1013] Recommendation ITU-T J.1013 （2020）, *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine.*

[b-ITU-T J.1014] Recommendation ITU-T J.1014 （2020）, *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities.*

[b-SG9 Report 17 Ann.1] ITU-T SG9 meeting report, SG9-R17-Annex 1 （2020）, Annex 1 to Report 17 of the SG9 fully virtual meeting held 16-23 April 2020.
https：//www.itu.int/md/T17-SG09-R-0017/en

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Available at： https：//movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

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，以及相关联的测量和测试
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
2020年，日内瓦