国　际　电　信　联　盟

ITU-T J.1015

(04/2020)

国际电信联盟
电信标准化部门

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

有条件访问和保护 – 可交换嵌入式有条件访问与数字版权管理解决方案

可交换有条件访问/数字版权管理（CA/DRM）解决方案的嵌入式通用接口（ECI）：高级安全系统 – 密钥阶梯块

ITU-T J.1015 建议书

国际电信联盟

ITU-T J.1015 建议书

可交换有条件访问/数字版权管理（CA/DRM）解决方案的嵌入式通用接口（ECI）：高级安全系统 – 密钥阶梯块

摘要

ITU-T J.1015建议书是一个系列的一部分，涵盖有关可交换有条件访问/数字版权管理（CA/DRM）解决方案规范的嵌入式通用接口（ECI）的高级安全系统密钥阶梯块。

本ITU-T建议书是ETSI标准[b-ETSI GS ECI 001-5-2]的转换，是ITU-T第9研究组与ETSI ISG ECI之间合作的结果。

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	2020-04-23	9	11.1002/1000/13576

关键词

有条件访问（CA）、数字版权管理（DRM）、交换

* 为获取本建议书，请在网页浏览器内键入URLhttp://handle.itu.int/，然后输入唯一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

引言

本ITU-T建议书[1]是ETSI标准[b-ETSI GS ECI 001-5-2]的转换，是ITU-T第9研究组与ETSI ISG ECI之间合作的结果。

本建议书的目的是促进电子通信服务、尤其是广播和视听设备市场的互操作性和竞争。然而，根据成员国的情况，还可以使用其他技术，这些技术也可能是适当的和有益的。

为了保护内容免受未授权访问，内容提供商对其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证内容解密密钥从**内容保护系统**到芯片组的传输安全。在本建议书中，芯片组内实施的协议步骤被称为“密钥阶梯”，本建议书规定了[b-ROEL]中展示的密钥建立协议的密钥阶梯。

密钥阶梯和该协议亦可用于保证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重加密的情况下，需要使用这类密钥。为此，芯片组可实施一次或多次内容加密操作。个人视频录制受保护内容，并将受保护内容导出至另一个不同的**内容保护系统**是典型的内容重加密使用案例。在本建议书中，内容解密密钥和内容加密密钥皆称为**控制字**（CW）。

本建议书亦规定了一种认证机制。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。

本建议书中规定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。

认证机构负责管理本建议书规定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撤销信息。然后，**内容提供商**将该证书和证书撤销信息作为输入信息用于其合规的**内容保护系统**；如第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I确定了一些有待进一步发展的领域。

[2] 在本建议书的文本中，使用黑体字来表示具有特定于嵌入式通用接口上下文的定义的术语，它们可能与通常用法有所不同。

ITU-T J.1015 建议书

可交换有条件访问/数字版权管理（CA/DRM）解决方案的嵌入式通用接口（ECI）：高级安全系统 – 密钥阶梯块

1 范围

本建议书规定了一种在**内容接收器**芯片组中实施的密钥阶梯块。该密钥阶梯块由一个保证**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。本建议书亦规定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。

[ISO/IEC 9797-1] ISO/IEC 9797-1:2011，信息技术 – 安全技术 – 消息认证码（MAC） – 第1部分：使用块密码的机制。

[IETF RFC 8017] IETF RFC 8017 (2016)，PKCS #1：RSA密码规范版本2.2。

[NIST FIPS 180-4] NIST FIPS PUB 180-4 (2015)，安全散列标准（SHS）。

[NIST FIPS 197] NIST FIPS PUB 197 (2001)，高级加密标准（AES）规范。

[NIST SP 800-107] NIST SP 800-107 修订1 (2012)，有关使用经批准之散列算法的应用程序的建议书。

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 认证机构（certification authority）：指的是负责在嵌入式通用接口（**ECI**）**生态系统**中管理公钥证书的一方。认证机构受到系统中所有其他方的信任，可以执行与证书关联的各项操作。

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

3.2.3 内容保护系统（content protection system）：指的是**ECI生态系统**中的系统，它采用加密技术来对内容和服务的访问。该术语可能常会与另一个术语“服务保护系统”交替使用。这类典型系统为管理有条件访问（CA）系统或数字版权管理（DRM）系统。

3.2.4 内容提供商（content provider）：将数字内容分发到**ECI生态系统**中**内容接收器**的一方。

3.2.5 内容接收器（content receiver）：用于访问**ECI生态系统**中数字内容的设备。**内容接收器**包含带有**内容解扰器**的芯片组。

3.2.6 内容解扰器（content descrambler）：ECI生态系统芯片组中能够解密内容的组件。内容解扰器也可能能够加密内容（出于内容重加密的目的）。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（control word）：用于加密和解密**ECI生态系统**中内容的秘密密钥。在数字版权管理系统中，控制字通常称为内容密钥。

3.2.8 加密散列函数（cryptographic hash function）：ECI生态系统中的非密钥加密函数，它将任意大小的数据（称为消息）作为输入，并生成固定大小的输出数据块（称为消息摘要）。本建议书中假定的**密码散列函数**的属性是：**密码散列函数**表现为一个随机函数，并且具有第二原像抗性。

3.2.9 数字签名方案（digital signature scheme）：密钥非对称加密方案，用于保护**ECI生态系统**中的数据真实性。**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。密钥生成为（秘密/私钥，公钥）对。使用秘密/私钥对数据进行签名，并使用相应的公钥来验证签名。本建议书规定的**数字签名方案**用于保护[b-ROEL]中定义的消息的真实性；特别是，该方案在本建议书中不用于提供不可否认性或来源认证。

3.2.10 ECI生态系统（ECI ecosystem）：由一个可信机构和若干个平台以及现场**ECI**兼容的客户驻地设备组成的商业运营环境。

3.2.11 消息认证码算法（message authentication code algorithm）：密钥对称加密算法，用于保护**ECI生态系统**中的数据的真实性。**消息认证码算法**将消息和秘密密钥作为输入，并生成称为MAC的输出数据块。本建议书中规定的**消息认证码算法**用于将密文消息加密绑定到其相关数据；特别是，该算法在本建议书中不用于提供来源认证。

3.2.12 公钥加密方案（public-key encryption scheme）：密钥非对称加密方案，用于保护**ECI生态系统**中数据的机密性。**公钥加密方案**由密钥生成算法、加密操作和解密操作组成。密钥生成为（公钥，秘密/私钥）对。使用公钥对数据进行加密，并使用相应的秘密/私钥从密文中恢复数据。

3.2.13 对称加密方案（symmetric encryption scheme）：密钥对称加密方案，用于保护**ECI生态系统**中的数据机密性。**对称加密方案**由密钥生成算法、加密操作和解密操作组成。**对称加密方案**的加密和解密操作使用相同的密钥作为输入。

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：

AES	高级加密标准
AD1	关联数据1
AD2	关联数据2
AK	认证密钥
CA	有条件访问
CID	公司标识
CISSA	通用IPTV面向软件的加扰算法
CPU	中央处理单元
CSA	通用加扰算法
CPK	芯片组公钥
CSK	芯片组秘密密钥/私钥
CW	控制字
DRM	数字版权管理
DVB	数字视频广播
ECB	电码本
ECI	嵌入式通用接口
ECP	增强型内容保护
ID	标识符
LK	链路密钥
MAC	消息认证码
MK	MAC密钥
OUI	组织唯一标识符
RSA	RSA公钥加密算法
SHA	安全散列算法
SIM	签名输入消息
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

本建议书中的黑体术语表示这些术语使用了ECI特殊定义，可能与它们的正常含义有所偏差。

6 芯片组ID和芯片组主密钥对

本条款介绍了合规芯片组个性化的各方面问题。每个合规芯片组皆与一个位串相关联，用于识别芯片组身份，即**芯片组ID**，以及芯片组主密钥对。

应向每个合规芯片组分配一个全球独一无二的64位**芯片组ID**。如果**芯片组ID**的各位从左至右编号为0至63，第i位（$0 \le i \le 63$）表示为b_i，则（b_0, b_1, b_2, b_3）应包含一个注册结构标识符。注册机构标识符的每个数值应最多与一家注册机构相关联。**芯片组ID**还应包含一个制造商标识符。一个合规芯片组的**芯片组ID**的注册机构标识符数值和芯片组制造商标识符应能独一无二地识别出生产该芯片组的芯片组制造商。另外，通过（b_0, b_1, b_2, b_3）的数值识别出的注册机构应管理可与该数值结合使用的芯片组制造商标识符的分配。

若$(b_0, b_1, b_2, b_3) = (0, 0, 0, 0)$，则IEEE注册机构（https://standards.ieee.org/develop/regauth/）应为该注册机构，24位的OUI（http://standards.ieee.org/develop/regauth/oui/）或24位的CID（http://standards.ieee.org/develop/regauth/cid/）应用于识别芯片组制造商。另外，若（b_0, b_1, b_2, b_3）=（0, 0, 0, 0），那么（$b_4, b_5, \cdots, b_{27}$）应包含OUI/CID，在OUI/CID的Octet 0中，b_4是最重要的一位（亦见[b-IEEE-OUI]），而b_{27}是OUI/CID的Octet 2中最不重要的一位。

注册机构标识符的所有其他数值可供未来使用。

芯片组主密钥对与一个公钥加密方案相关联，包括一个芯片组秘密密钥/私钥CSK和一个芯片组公钥CPK。如下文第7和8条所述，（CSK、CPK）是密钥阶梯和认证机制的主密钥对。第10.2条具体介绍了**公钥加密方案**和CSK与CPK的表示法。

一个合规的芯片组应能够生成自己的密钥对（CSK、CPK），防止CSK值被系统中的任何一方获悉。在这种情况下，只有**芯片组ID需要在个性化过程中被分配给芯片组，**且在这个分配过程中需保护**芯片组ID**的真实性。若芯片组没有生成自己的密钥对，那么应在（**芯片组ID**、CSK、CPK）被分配给芯片组的过程中保护（**芯片组ID**、CSK、CPK）的真实性和CSK的机密性。

用作（CSK, CPK）密钥对生成算法输入数据的随机数字应至少有128位熵。

一个合规芯片组应永久存储它的（**芯片组ID**、CSK、CPK），并采取措施保护被存储的CSK不被泄露，以及被存储的**芯片组ID**、CSK和CPK的完整性。

内容接收器的CPU应能够读取被存储的**芯片组ID**和被存储的芯片组公钥CPK。这使得**认证机构**能够把导出信息用作输入数据，给芯片组创建一个公钥证书。另外，导出的**芯片组ID**能够使**内容提供商**识别该芯片组及其证书。

认证机构应替它管理的每个芯片组维护（**芯片组ID**、CPK）。本建议书不排除在系统中出现一个以上**认证机构**的情况。在（**芯片组ID**、CPK）被分配给关联的一个或多个认证机构的过程中，应保护（**芯片组ID**、CPK）的真实性。

7 密钥阶梯

7.1 概述

本条介绍密钥阶梯的功能设计。在本建议书中，芯片组里实施密钥阶梯的数据块被称为密钥阶梯块。密钥阶梯如图7-1所示。正如第6条和上图所示，利用一个**芯片组ID**和一个芯片组秘密密钥/私钥CSK对芯片组进行个性化设置。

控制字是密钥阶梯块的一个输出信息，用CW表示，用于内容解密或内容加密。位串是密钥阶梯块的第二个输出信息，用CW-URI表示，它规定了CW的使用规则信息（CW-URI规范及相关使用规则参见第7.3.1条）。CW和CW-URI是**内容解扰器**（图7-1没有展示**内容解扰器**）的输入信息。

- 密钥阶梯块和内容解扰器应在单一硅片中执行。
- 若内容解扰器提供了一个访问内容接收器处理器的接口，使处理器可以将明文控制字发送至内容解扰器（即，绕过密钥阶梯块），那么，应可以永久禁止此项功能。
- 若密钥阶梯计算出一个控制字，那么应只有该密钥阶梯块和内容解扰器可以访问该控制字。
- 在将（CW, CW-URI）从密钥阶梯块分配至内容解扰器的过程中，应保护（CW、CW-URI）的真实性和控制字的机密性。

密钥阶梯块应与**内容接收器**的一个处理器相连接。例如，处理器可以是**内容接收器**的安全处理器，也可以是CPU。如第6条所述和图7-1所示，这个处理器能够读取**芯片组ID**。这使得**内容提供商**可以识别该芯片组，并从**认证机构**获得与CPK相对应的公钥证书。如第7.2条所述，要计算输入密钥阶梯的一条信息，需要获悉CPK的值。

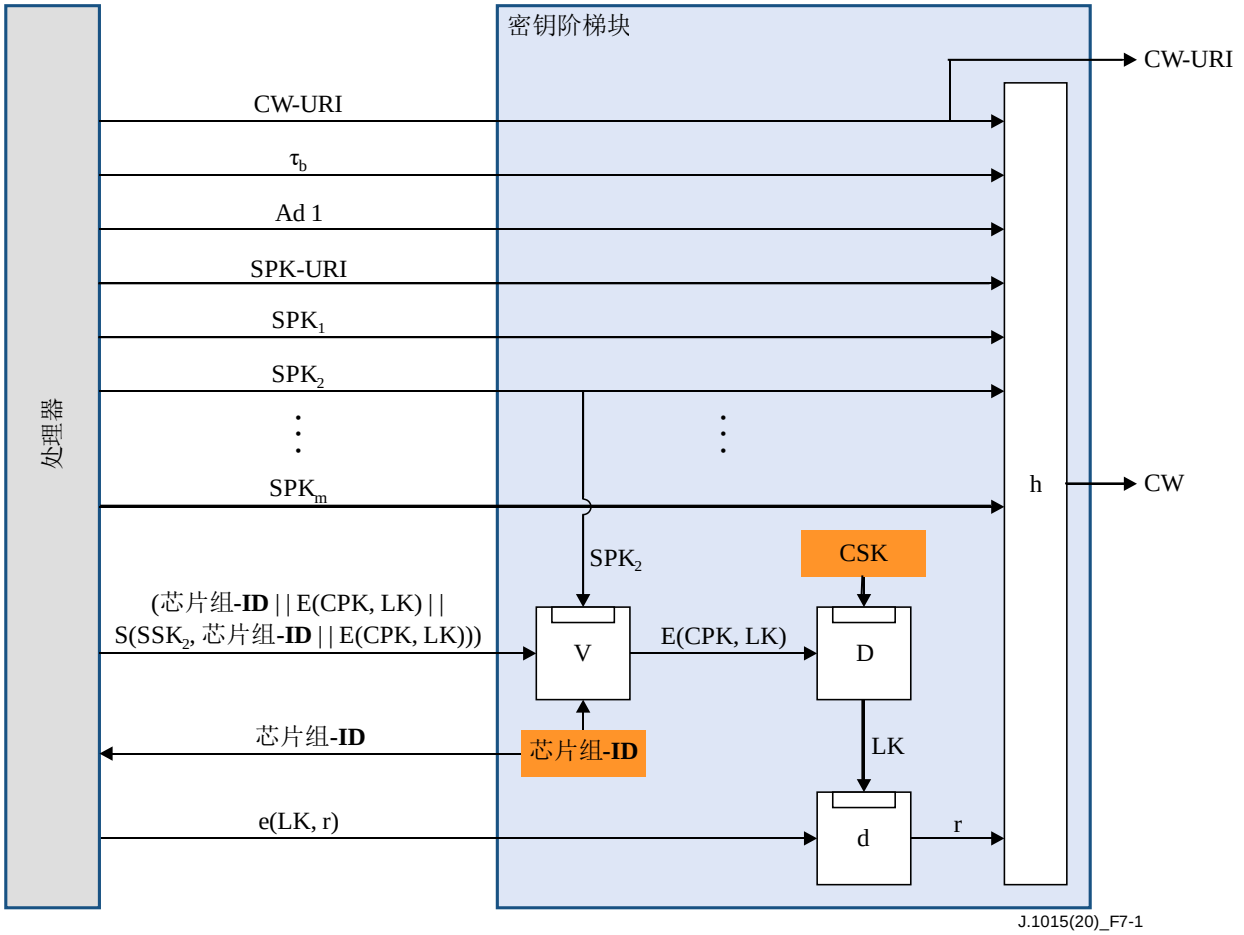

图7-1 – 密钥阶梯

如第6条所述，（CSK、CPK）与**公钥加密方案**相关联。相对应的加密和解密操作分别用E和D表示。E和D是键控密码操作，且每一个操作皆有两种输入信息：一个密钥输入和一个消息输入。本建议书假设键控密码操作或算法的第一个输入信息为密钥。

示例：使用E和芯片组公钥CPK加密的消息M被写作E(CPK, M)。

本建议书介绍的机制亦使用了一种**数字签名方案**；S和V分别表示签名生成操作和签名验证操作。**数字签名方案**的密钥对与发送方相关联，包括一个发送方秘密密钥/私钥SSK和一个发送方公钥SPK。本建议书假设发送方是一个**内容保护系统**。如图7-1所示，向密钥阶梯块输入了许多不同的SPK，用SPK_1、SPK_2...SPK_m ($m \geq 1$)表示。密钥阶梯块应支持各种m值的密钥阶梯，$1 \leq m \leq 16$。实际上，每个密钥对（SSK_i, SPK_i），其中$1 \leq i \leq m$，皆将与一个**内容保护系统**相关联；不过，也可以在多个系统之间共享此密钥对。

SPK-URI与SPK_1、SPK_2 ...SPK_m相关联。该密钥阶梯块输入信息定义了SPK_1、SPK_2 ...SPK_m的使用规则信息。第7.3.2条具体介绍了SPK-URI及相关使用规则。如图7-1所示，利用一个SPK和验证操作V来验证输入消息（**芯片组ID** || E(CPK, LK) || S(SSK_i, **芯片组ID** || E(CPK, LK))）的签名。在下列文本中，该输入消息也可表示为SIM_{KL}。图7-1假设$i = 2$，且SPK-URI及使用规则允许SPK_2被用于验证签名。

密钥阶梯还执行一种**对称加密方案**。该方案中的加密和解密操作分别用e和d表示。密钥阶梯将链路密钥LK用作该方案的密钥，随机数字*r*（或下文第7.4条介绍的另一种链路密钥）作为消息。随机数字*r*用位串表示，其长度应为128位。

最后，密钥阶梯块执行函数h。该函数以**加密散列函数**（参数h见第10.4条）为基础。

如图7-1所示，密钥阶梯块的另两个输入信息为τ_b和关联数据1；后者亦称为AD1。这两种输入皆可用位串表示：

- τ_b的长度应为8位。第7.5条规定了τ_b的使用。
- AD1的长度应为256位。AD1的内容参数不在本建议书范围之内，且本建议书假设密钥阶梯块除将AD1作为输入信息提供给h外，不对AD1进行处理。密钥阶梯块可将AD1或AD1的部分数据，以及CW-URI和CW传输给**内容解扰器**。

本建议书假设对称密钥、密文消息和签名用位串表示。第10规定了它们的长度。该条亦介绍了非对称密钥的表示法。

7.2 密钥阶梯计算

与密钥对（SSK_i, SPK_i）相关联的发送方，且$1 \le i \le m$，可以采用下列步骤创建签名输入消息SIM_{KL}，即：

（**芯片组ID** || E(CPK, LK) || S(SSKi, **芯片组ID** || E(CPK, LK))）

使用下列步骤。

计算SIM_{KL}（发送方）

1) 生成一个链路密钥LK。
2) 计算密文E(CPK, LK)。
3) 连接**芯片组ID**和E(CPK, LK)；产生的位串用（**芯片组ID** || E(CPK, LK)）表示。
4) 采用SSK_i对位串（**芯片组ID** || E(CPK, LK)）签名；签名用S(SSK_i, **芯片组ID** || E(CPK, LK))表示。
5) 将该签名附在位串（**芯片组ID** || E(CPK, LK)）之后。

在收到SIM_{KL}和发送方公钥SPK_i之后，密钥阶梯块需采取下列步骤检索LK（在图7-1中，假设前三步由V执行）。

计算LK（密钥阶梯块）

1) 验证收到的**芯片组ID**是否与存储的**芯片组ID**相同。若这两个值不同，则密钥阶梯块应中止该计算。

2) 检查SPK-URI和第7.3.2条中定义的使用规则是否允许V使用SPK_i去验证签名。若不允许，则密钥阶梯块应中止该计算。

3) 利用收到的SIM_{KL}和SPK_i验证签名。若签名无效，则密钥阶梯块应中止该计算。

4) 计算LK = D(CSK, E(CPK, LK))。

接下来，密钥阶梯块应使用LK来处理输入消息e(LK, r) （亦参见图7-1）。发送方可采用下列步骤创建本消息。

计算e(LK, *r*)（发送方）

1) 生成一个随机位串r。

2) 计算e(LK, *r*)。

在收到e(LK, *r*) 并计算LK之后，密钥阶梯块应采用下列步骤计算*r*（亦参见图7-1）。

计算*r*（密钥阶梯块）

1) *r* = d(LK, e(LK, *r*))。

接下来，密钥阶梯块应使用函数h来计算控制字CW。如图7-1所示，h的输入信息包括CW-URI、τ_b、AD1、SPK-URI、SPK_1、SPK_2 ...SPK_m，及*r*。执行密钥阶梯需确保，当CW从r衍生而来时，用于验证SIM_{KL}（或更准确来说，SIM_{KL}包含与随机数字r相关联的链路密钥）真实性的公钥作为SPK输入信息提供给h。然后，密钥阶梯块应把CW-URI和CW传输给**内容解扰器**。

7.3 使用规则信息

7.3.1 控制字使用规则信息

CW-URI的长度须为64位，且从左至右这些位的编号为0至63。根据下列使用规则，CW-URI的值定义了CW的允许使用情况（亦参见表7-1）：如果位值为1，那么允许这种规定的使用，否则，不允许。由**内容解扰器**负责执行此项使用规则。**内容解扰器**须忽略：

i) 留作供未来使用的位值；和

ii) 与**内容解扰器**不支持的执行情况相对应的位值。

表7-1 – 控制字使用规则信息清单

位编号	说明
0	加密
1	解密
2 … 7	留作供未来使用
8	数字视频广播（DVB）通用加扰算法2（CSA2）[b-ETSI TS 100289]
9	DVB CSA3 [b-ETSI TS 100 289]
10 … 15	留作供未来使用
16	DVB通用IPTV面向软件的加扰算法（CISSA）版本1 [b-ETSI TS 103127]
17 … 23	留作供未来使用
24	先进电视系统委员会通用加扰/解扰算法[b-ATSC A / 70-1]
25 … 31	留作供未来使用
32	通用加密方案 – cenc保护方案[b-ISO/IEC 23001-7]
33	通用加密方案 – cbc1保护方案[b-ISO/IEC 23001-7]
34	通用加密方案 – cens保护方案[b-ISO/IEC 23001-7]
35	通用加密方案 – cbcs保护方案[i b-ISO/IEC 23001-7
36 … 39	留作供未来使用
40	中国广播影视数字版权管理（ChinaDRM） – 密码块链接模式[b-GY/T 277-2014]
41	ChinaDRM – 计数器模式 [b-GY/T 277-2014]
42 … 63	留作供未来使用

7.3.2 发送方公钥使用规则信息

SPK-URI的长度应为64位，这些位从左至右的编号亦为0至63。表7-2给出了SPK-URI的定义。特别是，若SPK_1、SPK_2 ...和SPK_m与SPK-URI（如表7-2所示）一起作为输入信息提供给密钥阶梯，那么，SPK-URI的位0, 1, …, m-1及位16, 17, .., 16+m-1 被用于定义{SPK_1, SPK_2, ..., SPK_m}的两个子集：当且仅当位i-1的值等于1时，SPK_i (i = 1, 2, …, m) 才是第一个子集的一个元素；当且仅当位i+15的值等于1时，SPK_i才是第二个子集的一个元素。在下文中，这两个子集分别用S_1和S_2表示。利用这种表示法，密钥阶梯需应用下列使用规则：

SPK使用规则1：在密钥阶梯中，当且仅当$SPK_i \in S_1$时，允许V使用SPK_i来验证SIM_{KL}的签名。

密钥阶梯块应执行SPK使用规则1。

在内容重加密情况下使用集合S_2。若内容进行重加密，那么需要图7-1中描绘的两个输入集合：一个输入集合与用于内容解密的CW相关联，另一个输入集合与用于内容加密的CW相关联。在这种情况下，下列使用规则把这两个输入集合连接了起来：

SPK使用规则2：在密钥阶梯中，当且仅当$SPK_i \in S_2$，并与用于内容解密的CW相关联时，才允许V使用SPK_i来验证用于内容加密的CW的SIM_{KL}的签名。

若**内容解扰器**支持内容重加密，那么，密钥阶梯块应执行SPK使用规则2。若密钥阶梯块不执行该使用规则，那么该芯片组中的另一个组件需执行SPK使用规则2，且执行时需确保输入到函数h的SPK-URI的值等于用于执行SPK使用规则2的SPK-URI的值。

表7-2 – 发送方公钥使用规则信息的定义

位编号	说明
0	spk1_in_set1
1	spk2_in_set1
2	spk3_in_set1
…	…
15	spk16_in_set1
16	spk1_in_set2
17	spk2_in_set2
18	spk3_in_set2
…	…
31	spk16_in_set2
32 … 63	留作供未来使用

7.4 其他密钥层

7.4.1 概述

第7.1和7.2条中的说明假设密钥阶梯的一个密钥层与链路密钥相关联。密钥阶梯也应支持链路密钥的其他密钥层，如图7-2所示（该图仅描述了与本条讨论相关的密钥阶梯的构件块）。

如图7-2，用t表示密钥阶梯中链路密钥的数量。密钥阶梯块应支持所有值的t（$1 \le t \le 24$）所对应的密钥阶梯。注意，第7.1和7.2条所介绍的方案中，$t = 1$。

7.4.2 密钥阶梯计算

发送方可采用下列步骤生成密钥阶梯块的t输入消息。

计算$e(LK_1, LK_2)$、$e(LK_2, LK_3)$ …$e(LK_{t-1}, LK_t)$和$e(LK_t, r)$（发送方）

1) 生成链路密钥LK_i for $i = 1, 2, \ldots, t$，和一个随机位串r。

2) 计算$e(LK_{i-1}, LK_i)$ for $i = 2, 3, ..., t$。

3) 计算e(LK_t, r)。

在收到e(LK_1, LK_2)、e(LK_2, LK_3) … e(LK_{t-1}, LK_t)和e(LK_t, r)之后，密钥阶梯块应采用下列步骤计算r（亦参见图7-2）。

计算*r*（密钥阶梯块）

1) 计算LKi = d(LKi-1, e(LKi-1, LKi))，i = 2, 3, ..., t。

2) 计算r = d(LKt, e(LKt, r))。

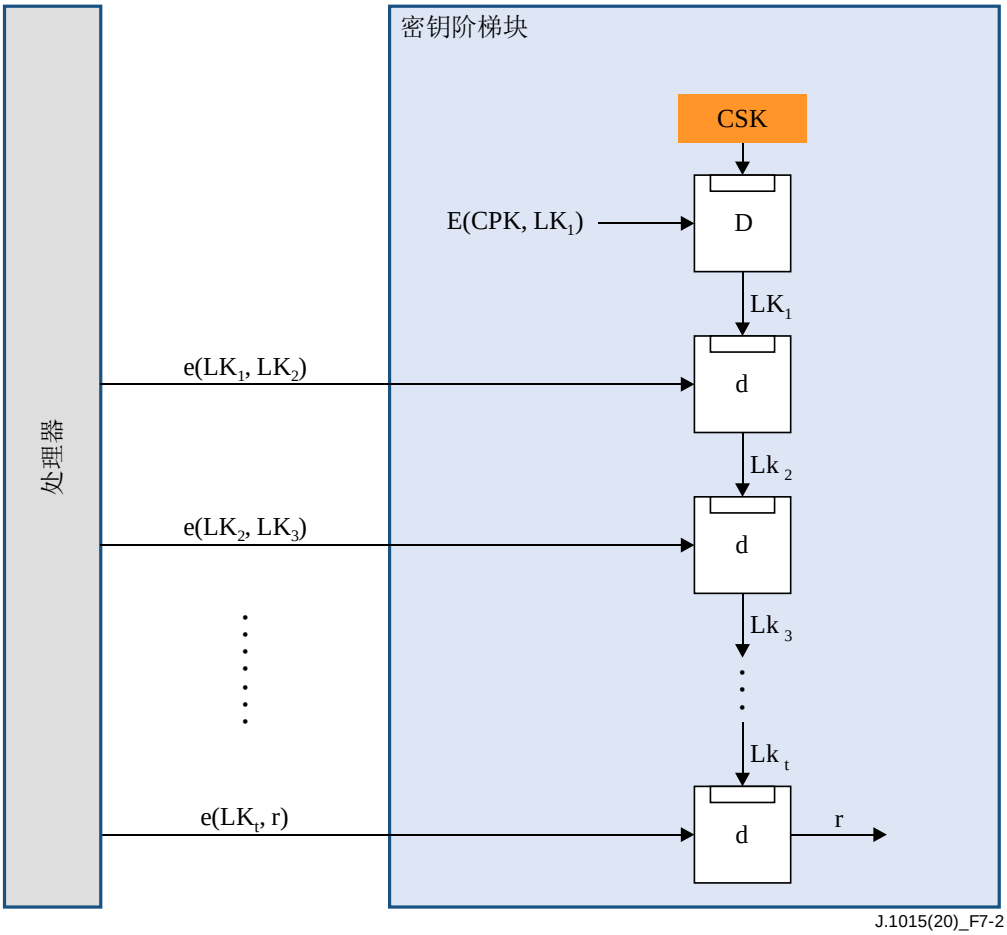

图7-2 – 其他密钥层

7.5 关联数据2

发送方可视情况将关联数据2（AD2）和e(LK_t, r)一起发送至密钥阶梯。位串τ_b的值（如第7.1条的介绍）表明AD2的存在。如第7.1条所述，τ_b的长度为8位。在下文中，τ为τ_b的整数表示，其中，τ的最低有效位相当于τ_b的最右位。密钥阶梯须支持$\tau \in \{0, 64, 96, 128\}$的所有值。若$\tau = 0$，则AD2不得存在，须采用第7.1至7.4条中介绍的方案。以下描述假设$\tau \neq 0$。在这种情况下，AD2须存在。若收到的$\tau \in \{64, 96, 128\}$，则密钥阶梯块须进行验证；若这种情况不适用，则密钥阶梯块须中止计算。

本建议书假设AD2表示为一个位串。用Len表示AD2的位长度。密钥阶梯块应支持Len的所有值（$1 \leq Len \leq 256$）。

用Len_b代表整数Len − 1的二进制表示，其中，Len_b的最右位相当于Len − 1的最低有效位。Len_b的长度应为8位。

在传输至密钥阶梯过程中，位串AD2应以加密形式与对应的密文$e(LK_t, r)$ 联系在一起。因此，发送方和密钥阶梯块应使用一种**消息认证码算法**，用mac表示。该算法的输入信息包括秘密MAC密钥MK、消息Len_b || $e(LK_t, r)$ || AD2，以及τ。mac的输出为长度为τ位的标签T。第10.5条详细介绍了mac算法。

用00…0表示128位的全零位串。发送方可采用下列步骤生成输入消息Len_b || $e(LK_t, r)$ || AD2 || T，发送至密钥阶梯（如图7-3所示）。

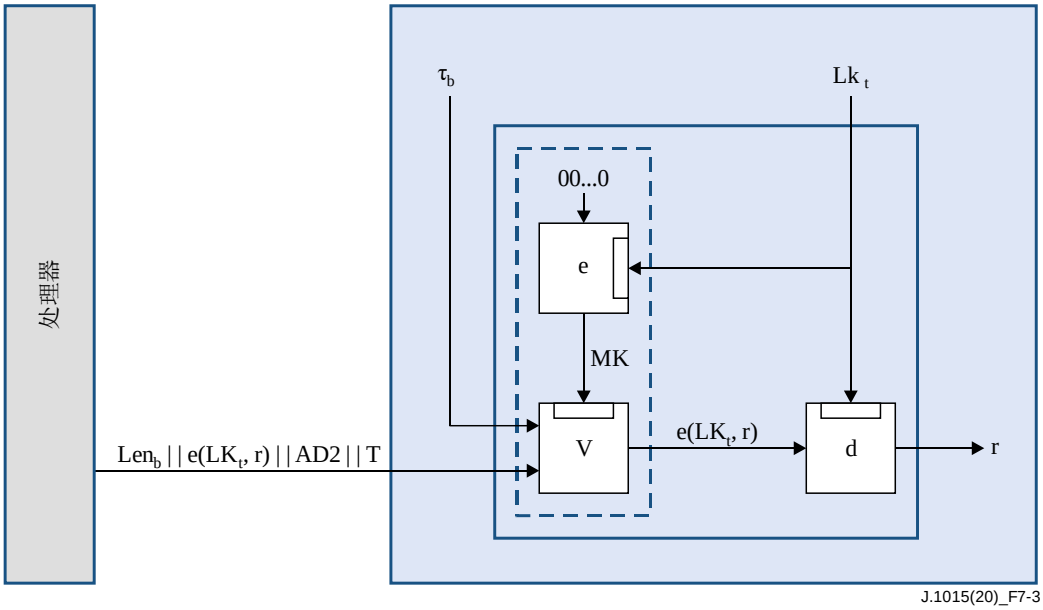

图7-3 – 关联数据2

计算Len_b || $e(LK_t, r)$ || AD2 || T（发送方）

1) 计算MK = $e(LK_t, 00…0)$。

2) 给位串$e(LK_t, r)$ || AD2预先加上Len_b。

3) 计算T = $mac(MK, Len_b || e(LK_t, r) || AD2, \tau)$。

4) 给位串Len_b|| $e(LK_t, r)$ || AD2加上T。

若τ = 0，则用消息Len_b || $e(LK_t, r)$ || AD2 || T 代替被使用的消息 $e(LK_t, r)$。在收到Len_b || $e(LK_t, r)$ || AD2 || T之后，密钥阶梯块应采用下列步骤（在图7-3中，用v表示第2 – 4步）计算$e(LK_t, r)$。

计算$e(LK_t, r)$（密钥阶梯块）

1) 计算MK = $e(LK_t, 00…0)$。

2) 计算T = $mac(MK, Len_b || e(LK_t, r) || AD2, \tau)$。

3) 验证收到的T是否等于计算出来的T。若这两个值不相等，那么密钥阶梯块应中止计算。

4) 从收到的消息中检索$e(LK_t, r)$。

AD2的内容说明不在本建议书范围之内，且本建议书假设密钥阶梯块没有处理AD2，而是将它作为mac算法的输入信息。密钥阶梯块可以将AD2或者AD2部分内容与CW-URI和CW一起传输至**内容解扰器**。

若$\tau \neq 0$，那么密钥阶梯的执行应确保，若CW衍生自r，那么与$Len_b \| e(LK_t, r) \| AD2$ 一起作为输入信息提供给mac算法的τ_b值，也作为输入信息提供给了h。

只有密钥阶梯块才能访问明文CSK、LK_i $(1 \leq i \leq t)$、MK和 r。

8 认证机制

8.1 概述

本条款介绍密钥阶梯块中认证机制的功能性设计。图8-1展示了该认证机制。该机制与密钥阶梯密切相关，如第7条所述；尤其是，它采用了相同的操作V、D和函数h，并且使用了相同的**芯片组ID**和CSK。但是，该认证机制并未使用链路密钥和CW-URI，SPK-URI和τ_b也不是该认证机制和函数h的输入信息。另外，h的输出内容不是一个用于内容解密或内容加密的控制字CW（特别是，该认证机制没有与**内容解扰器**直接连接），而是一个认证密钥AK。AK是一个与密钥阶梯中使用的**对称加密方案所属**相同的密钥。如图8-1所示，在认证机制执行过程中，仅使用了它的解密操作d。

输入消息（**芯片组ID** $\|$ E(CPK, r) $\|$ S(SSK_i, **芯片组ID** $\|$ E(CPK, r))）在下文中亦用SIM_{AUTH}表示。

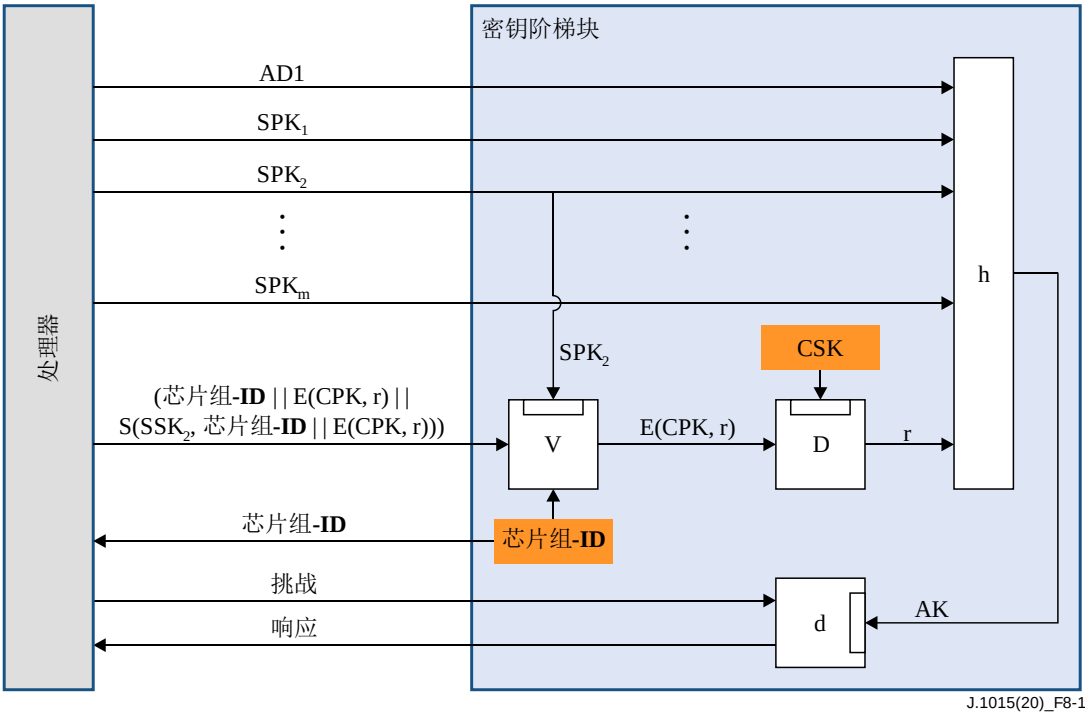

图8-1 – 认证机制

8.2 认证机制计算

与密钥对（SSK_i ,SPK_i） （$1 \le i \le m$）相关联的发送方可采用下列步骤创建签名输入消息SIM_{AUTH}，即

（**芯片组ID** || E(CPK, r) || S(SSKi, **芯片组ID** || E(CPK, r))），

计算SIM_{AUTH}（发送方）

1) 生成一个随机位串r。

2) 计算密文E(CPK, r)。

3) 连接**芯片组ID**和E(CPK, *r*)；产生的位串用（**芯片组ID** || E(CPK, *r*)）表示。

4) 采用SSK_i给消息（**芯片组ID** || E(CPK, r)) 签名；签名用S(SSK_i, **芯片组ID** || E(CPK, *r*)）表示。

5) 将该签名附加在位串（**芯片组ID** || E(CPK, *r*)）之后。

在收到SIM_{AUTH}和发送方公钥SPK_i之后，密钥阶梯块应执行下列步骤检索*r*（在图8-1中，前两步用V表示）。

计算*r*（密钥阶梯块）

1) 验证收到的**芯片组ID**是否等于存储的**芯片组ID**。若不相等，密钥阶梯块中止计算。

2) 利用收到的SIM_{AUTH}和SPK_i去验证签名。若签名无效，那么密钥阶梯块应中止计算。

3) 计算r = D(CSK, E(CPK, *r*))。

就认证机制而言，允许V使用任何SPK_i（$1 \le i \le m$）去验证SIM_{AUTH}的签名（在图8-1中，假设$i = 2$）。

接下来，应把AD1、SPK_1、SPK_2 ... SPK_m和r作为输入信息提供给函数h。h的输出结果即为认证密钥AK。认证机制在执行过程中需确保，当AK衍生于r时，用于验证SIM_{AUTH}（或者更准确地说，SIM_{AUTH}包含随机数字r）真实性的公钥，作为SPK输入信息之一提供给h。

然后，发送方可创建一条输入消息，称为“挑战”（Challenge）。从处理器收到挑战后，该认证机制需采用下列步骤计算响应。

计算响应（密钥阶梯块）

1) 计算响应= d（AK, 挑战）。

如图8-1所示，认证机制应将响应返回至处理器。

只有密钥阶梯块才能访问明文AK。

9 数据转换原语

9.1 BS2OSP

位串到八位组串的转换原语BS2OSP用于定义第10.2条中的**公钥加密方案**和第10.3条中的**数字签名方案**。

函数: BS2OSP(x)

输入: x 一个长度为8j（$j \geq 1$）的位串。

输出: X 一个长度为j的八位组串。

步骤:

1) 用x_i表示一个位（$0 \leq i \leq 8j\text{-}1$），且$x = x_0 x_1 \ldots x_{8j-1}$。

2) 用X_i表示一个由 $X_i = x_{8i+1} \ldots x_{8i+7}$（$0 \leq i \leq j\text{-}1$）定义的八位。

3) 输出八位组串$X = X_0 X_1 \ldots X_{j-1}$。

9.2 OS2BSP

八位组串到位串的转换原语OS2BSP用于定义第9.3条中的I2BSP原语和第10.2条中的**公钥加密方案**。

函数: OS2BSP(X)

输入: X 一个长度为j（$j \geq 1$）的八位组串。

输出: x 一个长度为8j的位串。

步骤:

1) 用X_i表示一个八位（$0 \leq i \leq j\text{-}1$）且$X = X_0 X_1 \ldots X_{j-1}$。

2) 用x_i表示一个位（$0 \leq i \leq 8j\text{-}1$），且这些位定义为$X_i = x_{8i+1} \ldots x_{8i+7}$（$0 \leq i \leq j\text{-}1$）。

3) 输出位串$x = x_0 x_1 \ldots x_{8j-1}$。

9.3 I2BSP

整数到位串的转换原语I2BSP用于定义第10.4条中的函数h。

函数: I2BSP(x)

输入: x 一个2048位的整数。

输出: 一个长度为2048的位串。

步骤: 若整数到八位组串的数据转换原语I2OSP(x, xLen)如[IETF RFC 8017]所定义，那么I2BSP(x) = OS2BSP(I2OSP(x, 256))。

10 密码操作

10.1 对称加密方案

密钥阶梯块中使用的**对称加密方案**须为电码本（ECB）操作模式的高级加密标准-128（AES-128）[NIST FIPS 197]。

10.2 公钥加密方案

公钥加密方案应为RSAES-PKCS1-v1_5 [IETF RFC 8017]。该方案包括一个加密操作和一个解密操作。根据7和8条，密钥阶梯块中仅执行解密操作，而发送方系统执行加密操作。

在[IETF RFC 8017]中，芯片组公钥CPK应等于接收方的RSA公钥 (*n*, *e*)。在本建议书中，*n*的位长应为2048，即，*n*的八位组长度，在[IETF RFC 8017]中用*k*表示，等于256。在[IETF RFC 8017]中，秘密密钥/私钥CSK应等于接收方的RSA私钥*K*。CSK的表示应等于[IETF RFC 8017]中的*K*的一个表示。

在[IETF RFC 8017]中，待加密的消息用*M*表示并作为一个八位组串。在本建议书中*M*的定义分别为：在密钥阶梯情况下，*M* = BS2OSP(LK)，在认证机制情况下，*M* = BS2OSP(r)。所以，在本建议书中，*M*的八位组长度等于16。

CPK和*M*是加密操作的输入信息：

RSAES-PKCS1-v1_5-Encrypt(CPK, *M*)。

该操作的输出信息是一份密文，用*C*表示，且在[IETF RFC 8017]中表示为一个八位组串。在本建议书中，*C*的八位组长度等于256。在密钥阶梯中，*C*等于BS2OSP(E(CPK, LK))，在认证机制中，等于BS2OSP(E(CPK, r))。

CSK和*C*是解密操作的输入信息：

RSAES-PKCS-v1_5-Decrypt(CSK, *C*)。

该操作在密钥阶梯块中执行。该操作的输出信息是消息*M*，代表一个八位组串。接下来，在密钥阶梯中，密钥阶梯块应计算LK = OS2BSP(*M*) ，在认证机制中，r = OS2BSP(*M*)。

10.3 数字签名方案

数字签名方案应为RSASSA-PKCS1-v1_5 [IETF RFC 8017]。该方案包括一个签名生成操作和一个签名验证操作。根据第7和8条，在密钥阶梯块中仅执行签名验证操作，而由发送方系统执行签名生成操作。

签名者的RSA公钥用 (*n*, *e*)表示，并在[IETF RFC 8017]中作为一对整数。在本建议书中，签名者的RSA公钥的模数*n*的长度应为2048位，即，*n*的八位组长度，在[IETF RFC 8017]中用*k*表示，等于256。进一步说，在本建议书中，公共指数*e*的值应等于$2^{16} + 1$。一个合规的芯片组应永久存储该值，且该芯片组应采取措施保护这个值的完整性。发送方的公钥SPK应等于模数*n*，意味着SPK的长度为2048位，且SPK是一个整数。在[IETF RFC 8017]中，发送方的秘密密钥/私钥SSK应等于签名者的RSA私钥*K*。

在[IETF RFC 8017]中，待签名的消息用*M*表示，并作为一个八位组串。在本建议书中，*M*的定义如下：

在密钥阶梯情况下，

$$M = \text{BS2OSP}（\textbf{芯片组ID} \parallel \text{E(CPK, LK)}）$$

在认证机制情况下，

$$M = \text{BS2OSP}（\textbf{芯片组ID} \parallel \text{E(CPK, r)}）$$

因此，在这两种情况下，*M*的八位组长度等于8 + 256 = 264。

SSK和*M*是签名生成操作的输入信息：

RSASSA-PKCS1-v1_5-Sign(SSK, *M*)。

在[IETF RFC 8017]中，签名生成操作的输出信息是一个签名，用*S*表示并作为一个八位组串。在本建议书中，*S*的八位组长度等于256。在密钥阶梯情况下，*S*等于BS2OSP(S(SSK$_i$, **芯片组ID** || E(CPK, LK)))，在验证机制情况下，等于BS2OSP(S(SSK$_i$, **芯片组ID** || E(CPK, r)))。

(SPK, $2^{16} + 1$)，*M*和*S*是签名验证操作的输入信息：

RSAES-PKCS-v1_5-Verify((SPK, $2^{16} + 1$), *M*, *S*)。

该操作在密钥阶梯块中执行。该操作的输出信息为“有效签名”或“无效签名”。

10.4 函数h

本条款详细介绍函数h。根据第7和8条，h的输入信息包括：

- 在密钥阶梯情况下：CW-URI, τ_b, AD1, SPK-URI, SPK$_1$, SPK$_2$, ..., SPK$_m$，及r。
- 在认证机制情况下：AD1, SPK$_1$, SPK$_2$, ..., SPK$_m$,及r。

若密钥阶梯块没有收到这两组输入信息中的任意一组，或者一组输入信息的长度不符合本建议书的规定，那么，密钥阶梯块应中止计算。否则，h应首先对它的每一个SPK输入信息应用I2BSP数据转换原语。然后，h应把代表着它的输入信息的位串连接起来（如下），以获取消息*M*。在密钥阶梯情况下：

$M = r \parallel \text{CW-URI} \parallel \tau_b \parallel \text{AD1} \parallel \text{SPK-URI} \parallel \text{I2BSP(SPK}_1\text{)} \parallel \text{I2BSP(SPK}_2\text{)} \parallel ... \parallel \text{I2BSP(SPK}_m\text{)}$，

在认证机制情况下：

$$M = r \parallel \text{AD1} \parallel \text{I2BSP(SPK}_1\text{)} \parallel \text{I2BSP(SPK}_2\text{)} \parallel ... \parallel \text{I2BSP(SPK}_m\text{)}。$$

忆及r、CW-URI、τ_b、AD1、SPK-URI及I2BSP(SPK$_i$)的长度分别为128位、64位、8位、256位、64位和2048位。因此，*M*的位长，在[NIST FIPS 180-4]中用*l*表示：在密钥阶梯情况下，等于520 + 2048*m*，其中*m*为消息块*M*中I2BSP(SPK$_m$)元素的数量，在认证机制情况下，等于384 + 2048*m*。

然后，h应计算SHA-256(*M*)，如[NIST FIPS 180-4]所定义的。

在认证机制情况下，h应把该256位消息摘要截断为128位，且输出该截断后的消息摘要。在密钥阶梯情况下，密钥阶梯块应把SHA-256的256位输出结果传输给**内容解扰器**，且，如果CW的长度为N位，那么，**内容解扰器**应把该输出结果截断至 N位。在这两种情况下，均应采用[NIST SP 800-107]中定义的截断方法。

10.5 消息认证码算法

如第7.5条所介绍，本条款定义了MAC算法。该**消息认证码算法**的定义见 [ISO/IEC 9797-1]，以下为部分节选：

- 块密码应为AES-128。
- 应采用填充方法3进行消息填充。该方法需要未填充消息$e(LK_t, r) \| A$的位长。该位长等于Len + 129。
- 应采用MAC算法1，利用消息和秘密密钥来计算MAC。
- MAC的长度应为τ位。

附录 I

有待进一步发展的领域

（本附录非本建议书不可分割的组成部分。）

已经确定，本建议书需要做进一步的开发和验证，才能满足[b- ITU-T J.1010]中规定的要求，并且[b-ITU-T J.1010]需要进行更新，以反映MovieLabs增强型内容保护（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[b-ITU-T J.1015.1]建议书未来应予更新，以反映对[b-ITU-T J.1010]的那些更新。

国际电联的许多成员国以及各行各业的利益攸关方 – 包括设备和电子组件的制造商、受版权保护的内容的所有者和被许可者、机顶盒（OTT）和线性电视服务的提供商以及全球各地基于有条件访问系统（CAS）和数字版权管理（DRM）解决方案的提供商都对嵌入式通用接口（ECI）不能完全满足ECP要求以及更广泛的行业内容保护要求表示了担忧。

更具体地说，其对ITU-T第9研究组（SG9）会议（2020年4月16-23日）的文稿引起了人们的关注。来自以色列、澳大利亚、ITU-T部门成员三星公司以及SG9准成员Sky Group和MovieLabs的文稿提议在ECI建议书中纳入一系列更改，但未就此达成共识。这些项目在[b-SG9 Report 17 Ann.1]中进行了清点。

这些建议包括：

1) 通过缩小ECI范围来简化ECI系统；

2) 取消DRM；

3) 取消对内容的重加密；

4) 取消软件管理；

5) 增加用于安全存储和加密操作的API；

6) 允许供应商特定的密钥阶梯；

7) 采用ITU-T J.1207 TEE要求；

8) 包括VM的TEE实施方案；

9) 升级密码算法的强度，例如，使用SHA-384；

10) 使用标准证书，例如，ITU-T X.509；

11) 重新考虑客户端之间的通信；

12) 与ETSI进行其他联络；

13) 进行额外的同行评审；

14) 探索信托机构模型的替代方案；

15) 进一步定义ECI合规性和稳健性规则的技术方面问题；

16) 增加有关多样性的要求，例如，地址空间随机化；

17) 增加有关运行时完整性检查的要求。

这些建议反映出内容保护及其违背之可能带来的威胁正在不断演变。ECI最初是在批准本ITU-T建议书之前近十年来构思的。对像ECI这样的系统，需要定期根据攻击技术和行业保护要求的最新状况进行评估。

存在其他机制以实现互操作性。特别是对DRM用例，大多数互联网视频服务已经部署了其他解决方案，以提供互操作性并满足其需求。

由于许多成员国将国际电联标准视为对其市场和行业发展有影响力的指导来源，因此进一步的澄清很重要。关注清单确保ECI在其国内市场中的实施，这可涉及对本ITU T建议书含义的全面理解，并确保在考虑立法、法规或有关要求消费者数字电视设备可互操作的市场需求时能虑及这些问题。它还确保技术设备制造商（它们可能更喜欢使用一组独特的要求或其他标准来设计产品）在为不同市场开发产品时可以考虑到这些问题。

参考书目

[b-ITU-T J.1010] ITU-T J.1010建议书（2016年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；用例和要求。

[b-ITU-T J.1011] ITU-T J.1011建议书（2016年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；体系结构、定义和概述。

[b-ITU-T J.1012] ITU-T J.1012建议书（2020年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；CA/DRM容器、加载程序、接口、撤销。

[b-ITU-T J.1013] ITU-T J.1013建议书（2020年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；虚拟机。

[b-ITU-T J.1014] ITU-T J.1014建议书（2020年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；高级安全性 – ECI特定功能。

[b-ITU-T J.1015.1] ITU-T J.1015.1建议书（2020年），可交换CA/DRM解决方案的嵌入式通用接口（ECI）；高级安全系统 – 密钥阶梯块：控制字使用规则信息及相关数据认证1。

[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-ISO/IEC 23001-7] ISO/IEC 23001-7:2016：信息技术 – MPEG系统技术 – 第7部分：基于ISO的媒体文件格式文件的通用加密。

[b-ATSC A/70-1] ATSC Standard A/70 Part 1:2010, *Conditional access system for terrestrial broadcast*. https://www.atsc.org/standard/a70-part-12010-conditional-access-system-for-terrestrial-broadcast/

[b-ETSI GS ECI 001-5-2] ETSI GS ECI 001-5-2 V1.1.1 (2017-07),*Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System; Sub-part 2: Key Ladder Block*. https://www.etsi.org/deliver/etsi_gs/ECI/001_099/0010502/01.01.01_60/gs_ECI0010502v010101p.pdf

[b-ETSI TS 100 289] ETSI TS 100 289 V1.1.1 (2011), *Digital video broadcasting (DVB); Support for use of the DVB scrambling algorithm version 3 within digital broadcasting systems*: https://www.etsi.org/deliver/etsi_ts/100200_100299/100289/01.01.01_60/ts_100289v010101p.pdf

[b-ETSI TS 103 127] ETSI TS 103 127 V1.1.1 (2013), *Digital video broadcasting (DVB); Content scrambling algorithms for DVB-IPTV services using MPEG2 transport streams*:

https://www.etsi.org/deliver/etsi_ts/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf

[b-GY/T 277-2014] ChinaDRM Lab, GY/T 277-2014: Technical specification for digital rights management for internet television.

[b-IEEE-OUI] IEEE Standards Association (2017), *Guidelines for use of extended unique identifier (EUI), organizationally unique identifier (OUI) and company ID (CID)*. https://standards.ieee.org/develop/regauth/tut/eui.pdf

[b-ROEL] Roelse, P. (2014). *A new key establishment protocol and its application in pay-TV systems*. https://arxiv.org/pdf/1308.4371.pdf

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 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