

ICS 33.040.40

M 32

YD

中华人民共和国通信行业标准

YD/T 2726-2014

IPTV 机顶盒技术要求 智能型

Technical specification on smart IPTV set-top box

2014-10-14 发布

2014-10-14 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语	3
5 概述	5
6 业务功能	5
6.1 基本要求	5
6.2 客户端应用	5
6.3 本地媒体播放	6
6.4 媒体共享	6
6.5 安全性要求	6
7 系统架构	6
8 硬件层	7
8.1 基本要求	7
8.2 外部接口	9
8.3 外围设备	10
8.4 电气性能	10
9 操作系统层	11
9.1 功能架构	11
9.2 协议支持	12
9.3 系统升级	13
9.4 系统开机	13
9.5 系统关机	14
9.6 操作要求	14
9.7 配置要求	14
10 应用层	15
10.1 应用层的内容	15
10.2 IPTV 应用	15
10.3 媒体共享	16
10.4 本地媒体	17

10.5 终端管理.....	17
10.6 其他应用.....	18
附录 A（资料性附录） 基于硬件 OTP 的终端安全保护方案.....	19
附录 B（资料性附录） 智能机顶盒 IPTV 业务功能实现 API.....	26

前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国电信集团公司、工业和信息化部电信研究院、中国联合网络通信集团有限公司、中兴通讯股份有限公司、华为技术有限公司、百视通网络电视技术发展有限责任公司、四川长虹电器股份有限公司、UT 斯达康（中国）有限公司。

本标准主要起草人：沈 昕、贾立鼎、胡冰松、朱良杰、张立杰、夏 俊。

IPTV机顶盒技术要求

智能型

1 范围

本标准规定了IPTV智能机顶盒终端的应用功能、操作要求、终端管理和接口要求等。

本标准适用于IPTV智能机顶盒。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB8898	音频、视频及类似电子设备 安全要求
GB13837	声音和电视广播接收机及有关设备无线电干扰特性 限值和测量方法
GB17625.1	电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)
GB/T 26683	地面数字电视接收器通用规范
YD/T 965	电信终端设备的安全要求和试验方法
YD/T 993	电信终端设备防雷技术要求及试验方法
YD/T 1654	IPTV 业务需求
YD/T 1696.1	机顶盒与 IPTV 业务平台接口技术要求 第 1 部分：总则
YD/T 1696.2	机顶盒与 IPTV 业务平台接口技术要求 第 2 部分：业务管理系统接口
YD/T 1696.3	机顶盒与 IPTV 业务平台接口技术要求 第 3 部分：业务导航系统接口
YD/T 1696.4	机顶盒与 IPTV 业务平台接口技术要求 第 4 部分：流媒体接口
YD/T 1696.5	机顶盒与 IPTV 业务平台接口技术要求 第 5 部分：终端管理接口
YD/T 1697	IPTV 内容运营平台与业务运营平台接口技术要求
YD/T 1823	IPTV 业务系统总体技术要求
YD/T 2016.3	IPTV 运维支撑管理接口技术要求 第 3 部分:终端
SJ/T10730-1997	VCD 视盘机通用规范
ITU-T Y.1901	支持 IPTV 业务的需求 (Requirements for the support of IPTV services)
IETF RFC 768	用户数据报协议 (User Datagram Protocol)
IETF RFC 791	IP 协议 (Internet Protocol)
IETF RFC 793	传输控制协议 (TCP) (Transmission Control Protocol)
IETF RFC 958	网络世界协议 (NTP) (Network Time Protocol)
IETF RFC 959	文件传输协议 (FTP) (File Transfer Protocol)
IETF RFC 1350	TFTP 协议 (Trivial File Transfer Protocol)
IETF RFC 1889	实时应用传输协议 (RTP) (A Transport Protocol for Real-Time Applications)
IETF RFC 2131	动态主机配置协议 (Dynamic Host Configuration Protocol)
IETF RFC 2236	因特网组管理协议版本 2 (Internet Group Management Protocol, Version 2)
IETF RFC 2312	S/MIME 第二版认证处理 (S/MIME Version 2 Certificate Handling)

IETF RFC 2326	实时流协议 (RTSP) (Real Time Streaming Protocol)
IETF RFC 2460	IPv6 协议 (Internet Protocol Version 6 (IPv6) Specification)
IETF RFC 2516	基于以太网传输 PPP 的方法 (A Method for Transmitting PPP Over Ethernet)
IETF RFC 2660	安全传输文本协议 (The Secure HyperText Transfer Protocol)
IETF RFC 2616	超文本传送协议 (HTTP) (Hypertext Transfer Protocol)
IETF RFC 3261	会话初始协议 (SIP) (Session Initiation Protocol)
IETF RFC 3550	实时传输协议 (RTP) (Real Time Control Protocol)
IETF RFC 3810	IPv6 状态中的组播听众发现版本 2(MLDv2) (Multicast Listener Discovery Version 2(MLDv2) for IPv6)
IETF RFC 3902	应用/soap+xml 媒体类型 (The Application/Soap+Xml Media Type)
IETF RFC 4443	ICMPv6 协议 (Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification)
ISO/IEC DIS 23009-1.2	HTTP 动态自适应流 (Dynamic adaptive streaming over HTTP (DASH))
ISO/IEC 29341	信息技术 UPnP 装置结构 (Information technology -- UPnP device architecture)
Apple Talk	ATF 文件协议 (Apple Talk File Protocol)
DLNA Architectures and Protocols	DLNA 导则 第 1 部分: 架构和协议 (DLNA Guidelines—Part 1: Architectures and Protocols)

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网协议电视 Internet Protocol Television, IPTV

IP网络上提供的多媒体业务(如电视/视频/音频/文字/图形/数据), 用于实现所需的QoS/QoE、安全性、交互性和可靠性。

3.2

终端用户 End User

产品或业务的实际用户。

3.3

IPTV 业务 IPTV Service

通过IP承载网络向用户提供能够支持交互能力的电视节目的直播、点播和时移播放等业务的总称。通过IPTV 业务, 用户可以得到高质量的数字媒体服务, 可以自由地选择视频节目, 实现媒体提供者和媒体消费者的实质性互动。

3.4

IPTV业务平台 IPTV Service Platform

业务平台包括业务管理系统、门户导航系统、媒体交付系统、运维支撑系统、安全管理系统和扩展业务系统, 机顶盒通过与这些系统的交互完成IPTV的内容管理和业务管理、认证、计费、鉴权以及流媒体的服务等功能。

3.5

电视直播 Linear TV

用户根据频道直接选择并收看电视节目，系统侧向选择该广播频道的全部用户同时推送相同的音视频流，播放既定的内容，为用户提供电视节目。

3.6

视频点播 Video on Demand

能向用户提供音视频存储内容的播放业务，用户可以对播放过程进行控制，控制包括快进、快退、重放等。

3.7

时移电视 Time-shift TV

对实时播放的广播频道进行短暂的暂停、倒退和快进操作的业务。

3.8

电子节目菜单 Electronic Program Guide

将所有数字电视节目按不同的分类规则组合在一起，用户通过遥控器就可以进行查看，也可以从电子节目单（EPG）中直接切换到正在播放的节目中去。

3.9

IPTV终端 IPTV Terminal

同时支持IPTV网络层和IPTV业务层接入的终端设备。IPTV终端通过与应用功能交互，获取EPG、内容版权许可证、密钥等业务信息；与内容分发平台交互，接受IPTV业务，完成解密和解码功能；并负责接收终端用户的控制指令。IPTV终端或者直接与电信网链接，或者通过家庭网关与电信网链接。

4 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用编程接口
APK	Android Package	安卓安装包
CBR	Constants Bit Rate	固定比特率
CLDC	Connected Limited Device Configuration	有限连接设备配置
CPU	Central Processing Unit	中央处理器
CSS	Cascading Style Sheets	层叠样式表单
DASH	Dynamic Adaptive Streaming over	动态自适应流
DES	Data Encryption Standard	数据加密标准
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DLNA	Digital Living Network Alliance	数字生活网络联盟
DMC	Digital Media Controller	数字媒体控制器
DMP	Digital Media Player	数字媒体播放器
DMR	Digital Media Receiver	数字媒体接收器
DMS	Digital Media Server	数字媒体服务器
DNS	Domain Name System	域名系统
DRM	Digital Rights Management	数字版权管理

DTS	Digital Theatre System	数字化影院系统
EPG	Electronic Programmer Guide	电子节目单
FTP	File Transfer Protocol	文件传输协议
HTML	Hypertext Markup Language	超文本标记语言
HTTP	Hypertext Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol Secure	安全超文本传输协议
ICMP	Internet Control Message Protocol	互联网控制报文协议
IGMP	Internet Group Management Protocol	互联网组管理协议
IN	Internal Number	内部编号
IP	Internet Protocol	网络协议
MAC	Media Access Control	媒体访问控制层
MLD	Multicast Listener Discover	组播侦听发现协议
MPEG	Moving Picture Experts Group	移动图像专家组
NTP	Network Time Protocol	网络时间协议
OS	Operating System	操作系统
OSS	Operation Support System	运营支撑系统
OTA	Over The Air	空中下载
OTP	One Time Programming	单次编程
PIM	Protocol Independent Multicast	协议无关组播
PPPoE	PPP over Ethernet	基于以太网点对点协议
RAM	Random Access Memory	随机存储器
RTCP	Real-time Transport Control Protocol	实时传输控制协议
RTP	Real-time Transport Protocol	实时传输协议
RTSP	Real-time Transport Streaming Protocol	实时传输流媒体协议
SD	Secure Digital Memory Card	安全数码卡
SIP	Session Initiation Protocol	起始会话协议
SN	Serial Number	序列号
S/N	Signal/Noise	信噪比
SOAP	Simple Object Access Protocol	简单对象访问协议
SSL	Secure Socket Layer	安全套接字层
STB	Set Top Box	机顶盒
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TM	Terminal Management	终端管理
TS	Transport Stream	传输流
UDP	User Datagram Protocol	用户数据报协议
UPnP	Universal Plug and Play	通用即插即用

USB	Universal Serial Bu	通用串行总线
VBR	Variable Bit Rate	动态比特率
XML	Extensible Markup Language	可扩展标记语言

5 概述

智能机顶盒是指具有智能操作系统，家庭网络中的一个应用设备，通过家庭网关访问专用网络，可通过直接连接电视机和音响等播放设备向用户提供页面信息浏览、视音频播放、应用、可视通信、媒体共享、游戏等交互式应用功能的多媒体终端。在本标准定义范围内所述STB或机顶盒，如无特殊说明，均指智能机顶盒。

智能机顶盒采用基于Linux的自由及开放源代码的操作系统，如Android、Meego、Bada等，具有如下特点：

——开放的框架：智能操作系统从高到低分为应用程序层、应用程序框架层、系统运行库层、系统核心层。核心层为上层系统提供内存管理、驱动模型等系统服务；包含多媒体引擎、浏览器引擎等的系统运行库层为平台提供了强大的功能。智能操作系统为应用程序提供了开放的运行化境，保证了所有运行程序访问底层框架能力的一致性，开发者可以使用应用程序框架提供的API进行应用程序的开发；

——自由下载应用：智能机顶盒允许用户自行下载安装和卸载软件、游戏等应用，通过应用程序的下载来扩充智能机顶盒的功能，提供给用户丰富的选择和体验，进而体现智能机顶盒的特点。

6 业务功能

6.1 基本要求

依据YD/T 1823中对于IPTV业务的定义，在本标准中所实现的智能机顶盒IPTV业务功能应满足以下标准中的相关要求：

- 基本业务：YD/T 1654中的相关要求，用于实现IPTV业务的基本业务功能；
- EPG页面展现：YD/T 1654中的相关要求，用于支持对于目前IPTV业务的显示及相关业务操作；
- 与IPTV业务能力平台的接口：YD/T 1697中对于业务认证、基本业务及增值业务访问、流媒体服务等相关功能的要求。

同时，还应该支持6.2~6.5的新增功能要求。

6.2 客户端应用

客户端业务功能是智能机顶盒支持各类应用客户端，包括应用商城客户端及IPTV等具体业务客户端。用户通过APP商城可以浏览商城内的客户端类业务，包括视频类、通信类、游戏类、音乐类、教育类、云存储、云空间等业务，并将客户端下载安装到“我的应用”等其他目录下，从而进一步实现相关应用。

客户端下载和升级要求如下：

- 下载：支持客户端下载进程的提示，如成功，则进一步提醒用户是否安装，如确认，则完成安装；如下载过程出现异常，提示用户并退出，不影响后续重新下载；
- 运行：下载后的客户端应用能够在机顶盒上运行并为用户提供相应业务功能；
- 升级：支持对需升级的应用客户端进行提示，用户确认后才可升级。支持升级进程的提示，包括下载和安装。如升级出现异常，提示用户并退出，不影响后续重新升级；
- 卸载：支持客户端的本地卸载，并在用户卸载时提示用户确认卸载。

6.3 本地媒体播放

本地媒体业务是指对本地存储设备内的视频、音频、图片等媒体文件进行浏览观看。智能机顶盒支持本地媒体业务的管理和播放功能，具体要求如下：

——视频文件播放：支持对于单个视频文件的单独播放或多个视频文件的顺序播放，在播放过程中支持视频文件的屏播放，并可在播放过程中对于进行 2X、4X、8X、16X、32X、64X（可选）倍速的快进快退、定位播放、退出等操作；

——音频文件播放：支持对于单个音频文件的单独播放或多个音频文件的顺序播放、随机播放、循环播放等。可支持在音乐播放过程中的图片播放功能，并允许用户配置播放的图片列表；

——图片文件播放：支持单个 1MB 大小图片文件的小尺寸预览及全屏播放，图片浏览中可支持背景音乐播放，并允许用户配置选择背景音乐的播放列表。在图片播放过程中，可支持多个图片文件的顺序播放、循环播放，并可设置自动播放的时间间隔。至少支持缩放、上升、擦除、下降、展开、淡入淡出等图片切换效果，并允许用户在多个图片的播放过程中进行暂停、恢复、退出等操作。

6.4 媒体共享

用户（此处指的用户仅特指家庭内部网络中多个终端的同一个持有者）可以通过不同终端（PC、手机、TV）在家庭内部进行视频、图片、文字等的媒体内容的展示、分享等活动。其业务功能包括（但不限于）以下功能：

——内容展现：用户可在当前使用的终端上查看家庭内部网络内终端间多媒体内容，并支持对于多媒体内容的分类；

——媒体播放：可以在当前使用的终端上进行家庭内部网络内终端间多媒体内容的播放、浏览、查看等操作。

6.5 安全性要求

智能机顶盒应能够保证其操作系统、应用安装/运行、用户业务账号等信息的安全性，可以通过采用硬件、软件的方式对于相关的信息进行保护。同时，对于机顶盒的业务认证、软件升级、应用下载等需提供认证的能力，以保证智能机顶盒的业务安全性。

7 系统架构

智能机顶盒主要包括硬件层、操作系统层和应用层，总体架构如图 1 所示。

在如图 1 所示的智能机顶盒所涉及的各层功能定义如下：

- 硬件层：主要包括智能机顶盒的基本硬件设备、硬件接口和外设。
- 操作系统层：主要包括驱动、各种函数库、应用 API 以及基本的可调用应用。根据其在操作系统运行过程中所起作用的不同，可分为：

——引导程序：普通域中的引导程序是机顶盒在启动过程中 CPU 执行的第一段片外代码，引导程序可根据不同的启动状态执行系统恢复程序或系统内核。

——系统恢复程序：可对系统内核、系统数据区、应用数据区进行升级、初始化等管理。

——系统内核：该部分执行后将系统引导到机顶盒的正常功能状态，在该状态下用户可通过机顶盒正常使用业务功能。

——系统数据区：是机顶盒最小的应用软件与数据存放区，机顶盒只能通过软件升级与恢复对系统数据区进行修改。

——应用数据区：是用户选装程序与数据的存放区域，机顶盒可在运行时对该区域进行修改操作。

- 应用层：主要包含了定制的管理客户端和业务应用客户端，包括 IPTV、终端管理、互联网音视频频等各类应用。

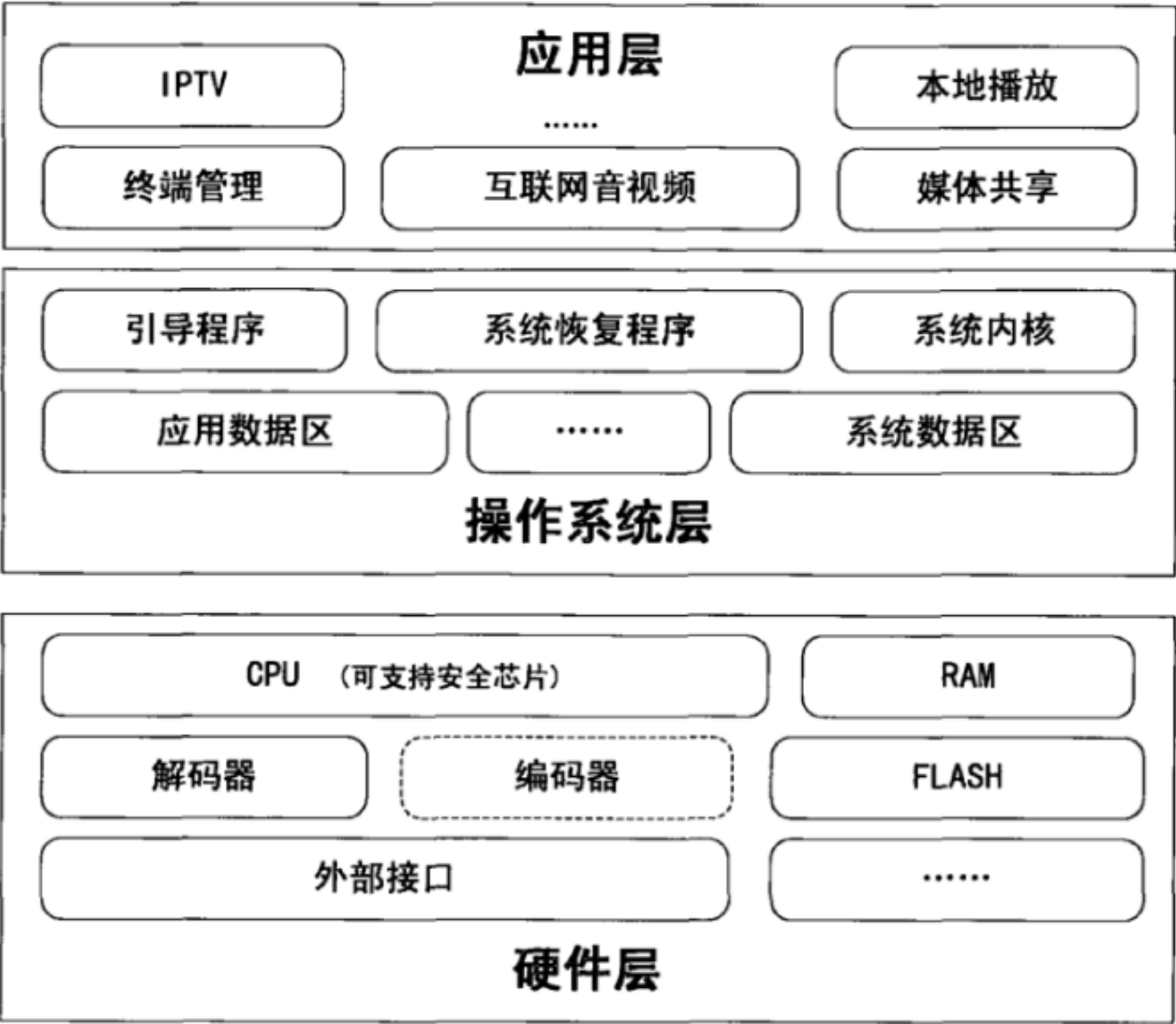


图 1 智能机顶盒总体架构

8 硬件层

8.1 基本要求

8.1.1 基本要求的内容

基本要求是指对于智能机顶盒硬件性能、编解码能力、面板、电源等硬件的要求，智能机顶盒的硬件应保证如下基本要求：

- CPU 主频：1GHz 以上；
- 内存：1G Byte 以上；
- Flash：2G Byte、4G Byte、8G Byte 及以上。FLASH 至少包括系统分区、应用分区、恢复分区等部分。建议系统分区在 300M Byte 以上，应用分区在 1G Byte 以上，恢复分区在 100M Byte 以上；
- 支持 3D 图形加速功能，要求达到 OpenGL_ES_2.0 以上标准；
- 机顶盒内部无风扇。

8.1.2 CPU

如需对于智能机顶盒操作系统、应用安装等的权限进行控制，对于 CPU 的要求参见附录 A.1。

8.1.3 解码

智能机顶盒具有的音视频解码能力见表 1。

表 1 音视频解码能力要求表

IPTV 解码	编码格式: H.264, MAIN/HIGH PROFILE @LEVEL 4.1 分辨率: 最大可达 1080P 编码模式: CBR/VBR 封装格式: TS 码流: 最大可达 20Mbit/s
3D 视频解码	编码格式: H.264, 3D 格式: FRAME COMPATIBLE 3D Format; FHD3D (可选) 分辨率: 最大可达 1080P 编码模式: CBR; 未来扩展支持 VBR 封装格式: TS 码流: 最大可达 20Mbit/s
基于 HTTP Streaming 的音视频服务及本地视频解码	编码格式: MPEG1、MPEG 2 MP@HL、MPEG4 、VC-1、WMV 7/8/9、DIVX/XVID、AVS jizhun (平滑支持)、RM/ RMVB (硬解可选, 软解必选), HIGH PROFILE@ LEVEL 4.1 分辨率: 最大可达 1080P 编码模式: CBR/VBR 封装格式: TS、MP4、MKV、AVI、RM/ RMVB (硬解可选, 软解必选)、FLV/F4V (硬解可选, 软解必选) 平均码率: 基于 HTTP Streaming 的音视频服务最大可达 20Mbit/s; 本地播放最大可达 40Mbit/s
音频解码	立体声要求: 要求支持 MPEG-1 LAYER 1/2、MPEG-1 layer 3、MPEG-2 AAC LC/MAIM、MPEG-4 AAC LC/MAIN、HE-AAC V1/V2、WAV、WMA、PCM 等格式 环绕声要求: 支持多音轨, 开机使用默认音轨
输出模式	HDMI1.3@1080P、1080i、720P、D1 ,机顶盒自动适应电视机模式输出

8.1.4 编码 (可选)

针对机顶盒支持视频通信功能时, 所需要的编码能力要求如下:

● 音视频编解码格式

——要求支持 G.711 A/U、iLBC、G.729 音频编解码, 以及 H.264 视频解码。

——机顶盒将音视频通过标准的 RTP 打包方式分别传送, 双方根据 SIP 协议协商的码率控制各自发送方码率。

● 视频编解码要求

采用 H.264 进行编解码时应符合以下要求:

——采用 BASELINE PROFILE 方式, 降低编码开销, 提高实时效率。

——采用 VBR、CBR 方式。

——使用 4:2:0 采样方式。

● 视频码流要求

——机顶盒在视频通话过程中的帧率及码率推荐值见表 2。

表 2 帧率及码流推荐表

屏幕分辨率	帧率(fps)	码率(kbit/s)
D1	22~25	660~950
720P	22~25	2400~3400
1080P	22~25	5350~7600

——机顶盒在各视频分辨率上的码流最大值不超过表 3 中规定的值：

表 3 针对不同分辨率的码流最大值表

分辨率	码率最大值
D1	2Mbit/s
720P	4Mbit/s
1080P	8Mbit/s

8.1.5 面板

机顶盒的面板应符合以下要求：

● 按键

具备【电源】（标示为：0 及 1，0 表示关机，1 表示开机）。

● 指示灯

指示灯应具备电源指示灯（必选）、红外指示灯（必选）及网络状态灯（可选）。

电源指示灯、红外指示灯为必选，指示灯位于前面板。电源指示灯的颜色标示为：开机后为绿色，待机为红色，亮度不影响用户夜间休息；红外指示灯：机顶盒响应遥控器操作，指示灯闪烁。

● 网络状态灯

正常状态为绿色，异常为红色。

8.2 外部接口

8.2.1 基本要求

外部接口是指智能机顶盒对外提供的媒体输出、网络接入、外设设备支持等的要求。所有硬件外部接口均应采用标准的字符、文字或图示等进行标示说明。

8.2.2 媒体接口

机顶盒必须支持以下媒体接口：

● 视频输出

——MINI CVBS 端子（可选）：用于复合视频输出，且在其他输出接口有效时有输出，接口颜色为黄色。

——HDMI 1.3 以上接口，为默认输出接口。

● 音频输出

——音频输出 SPDIF 接口（可选）。

8.2.3 外设接口

机顶盒必须支持的外设媒体接口如下：

——红外接口，用于接遥控器输入；

——USB 接口，符合 USB 2.0 标准；2 个（可支持三口以上 USB HUB），建议 4 个，最大电流 500mA，工作电压 5V，至少支持外接移动硬盘下载和播放以及外接 USB 摄像头、体感游戏手柄；

——SD 卡接口（可选），用于存储扩展；

——蓝牙接口（可选）。

8.2.4 网络接口

机顶盒必须支持的网络接口如下：

——有线网络接口：具备至少一个 RJ45 10/100BaseT 网络接口，且需有图示标识；

——无线网络接口（内置，可选）：要求无线网络接口支持 IEEE802.11b/g/n（2.4Gb/5.8Gb），5.8Gb 可选。

8.3 外围设备

8.3.1 普通遥控器

遥控器是用于控制机顶盒的红外无线发射装置。

- 基本要求

——遥控器对于机顶盒的有效操作距离必须在 8 米以上。

——遥控器有效操作角度为接收器中心线正负 60 度以上。

——遥控器面板需具有指示灯，在遥控器按键按下并将信号发送给机顶盒时，提示灯应闪烁。

——当遥控器正常工作时，不应影响其他设备；同时机顶盒也不能被其他设备的遥控器所影响。

- 遥控器识别

——机顶盒操作可由不同遥控器控制，根据接收到的遥控器用户码值识别遥控器类型。

——对于该功能要求机顶盒可通过软件升级方式支持不同类型的遥控器的使用。

8.3.2 融合遥控器（可选）

融合遥控器是指同时具备按键、体感、鼠标等功能，可替代普通遥控器操作现有 IPTV 业务，也可操作体感游戏的新型遥控器。

机顶盒可支持通过 USB 接口与融合遥控器的接收器相连接，同时需支持融合遥控器的即插即用等相关功能。

8.3.3 摄像头（可选）

机顶盒支持通过外置摄像头实现视频的采集和编码，摄像头将采集的视频内容编码后通过 USB 2.0 接口发送给机顶盒。机顶盒应至少支持 H.264 编码分辨率在 1280*720 以下摄像头设备。

8.4 电气性能

机顶盒在电气性能方面主要包括以下几个方面的要求：

- 音视频信号

机顶盒视频信号相关电气性能至少应符合以下要求：

——符合 GB/T 26683 的要求。

- 环境适应性

机顶盒至少支持以下环境适应性要求：

——应可适应温度为 $-10^{\circ}\text{C} \sim 40^{\circ}\text{C}$ 的环境；

——其他环境条件应符合 SJ/T10730-1997 第 5.7 节的规定。

- 安全性

机顶盒至少支持以下安全性要求：

——符合 YD/T 965 的要求；

——符合 YD/T 993 的要求；

——符合 GB8898 的要求。

- 可靠性

机顶盒至少支持以下可靠性要求：

- 支持平均无故障工作时间应大于 20000h;
- 支持在 20℃~30℃室温连续运行 48h 以上的情况下温度正常, 表面温度不超过 45℃。

● 供电

如使用外置电源适配器, 机顶盒至少支持以下供电要求:

- 支持设备电源模块的可靠性大于 99.99%;
- 则支持外加交流电通过外置适配器转为安全电压后接入 STB。

● 功耗

机顶盒支持以下功耗要求:

- 机顶盒在正常工作(播放本地移动硬盘中 40MBytes 的 1080P 视频内容)时的功耗不大于 15W; 播放 IPTV 平台高清视频时功耗不大于 10W;
- 待机时功耗不大于 1W。

● 噪声

机顶盒在工作时的噪声不应高于 30dBA。

● 电磁兼容性

- 符合 GB13837 及 GB17625.1 的要求。

9 操作系统层

9.1 功能架构

图2示出在智能机顶盒的智能操作系统上进行扩展以实现IPTV相关业务功能的系统架构。其中, 虚线左侧的部分是为实现此功能所进行的功能扩展(实现API参见附录B), 右侧部分为原有智能操作系统。

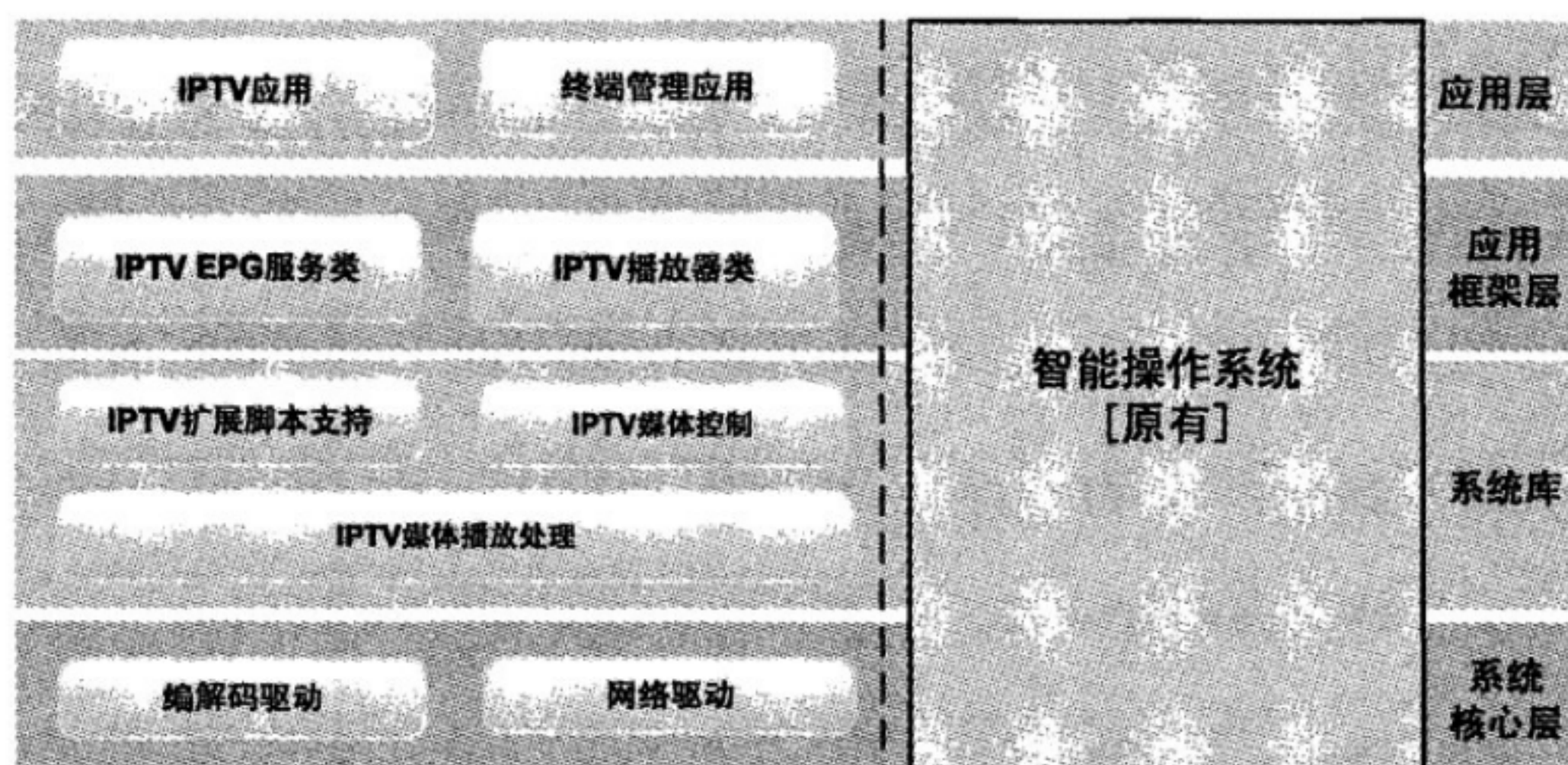


图2 智能机顶盒软件框架

如图2所示, 为支持IPTV应用及终端管理功能, 本标准定义在软件系统各层增加以下扩展功能模块及应用:

● 系统核心层扩展

——编解码驱动: 指由智能机顶盒提供方开发的硬件编/解码器驱动, 根据智能机顶盒使用的硬件主板所采用的硬件编/解码器, 提供符合智能机顶盒操作系统驱动架构的相应功能。

——网络驱动：指为支持 IPTV、视频通话等业务而扩展集成的网络驱动协议，包括 IGMP V2 等。

● 系统库扩展

——IPTV 扩展脚本支持：提供对浏览器进行扩展的能力，用于 IPTV 相关的扩展脚本的支持。参见附录 B。

——IPTV 媒体控制：该通过网络模块实现 IPTV 标准 RTSP/IGMP 流的获取、解析、TS 拆包、丢包重传等功能。参见附录 B。

——IPTV 媒体播放处理：IPTV 媒体控制获取到用户操作并对流媒体播放进行媒体解析后，将调用 IPTV 媒体播处理的相关方法控制解码器状态进行媒体播放的处理。参见附录 B。

● 应用框架扩展

——IPTV 播放器类：IPTV 业务的 JAVA 调用接口，封装了底层 IPTV 业务应用接口，并向应用层提供 JAVA 调用方法。

——IPTV EPG 服务类：IPTV 的 EPG 呈现类，封装了 EPG 呈现所需的应用接口。

9.2 协议支持

为实现相应业务功能的支持，智能机顶盒必须支持以下协议：

——DASH：见 ISO/IEC DIS 23009-1.2。

——DHCP：见 IETF RFC 2131。

——DHCP Option：见 IETF RFC 2312。

——DLNA（1.5 及扩展）：见 DLNA Architectures and Protocols。

——FTP：见 IETF RFC 959。

——HTTP（1.1 及以上）：见 IETF RFC 2616。

——HTTP-PD（HTTP STREAMING）：见 IETF RFC 2616。

——HTTPS：见 IETF RFC 2660。

——ICMPv6：见 IETF RFC 4443。

——IGMPv2：见 IETF RFC 2236。

——IP：见 IETF RFC 791。

——IPV6 PIM：见 IETF RFC 2460。

——MLDv2：见 IETF RFC 3810。

——NTP：见 IETF RFC 958。

——PPPoE：见 IETF RFC 2516。

——RTCP：见 IETF RFC 3550。

——RTMP：见 Apple Talk。

——RTP：见 IETF RFC 1889。

——RTSP：基本要求见 IETF RFC 2326。

——SIP：见 IETF RFC 3261。

——SOAP（1.0 及以上）：见 IETF RFC 3902。

——SSL2.0/3.0：见 IETF RFC 2660。

——TCP：见 IETF RFC 793。

- TFTP（可选）：见 IETF RFC1350。
- UDP：见 IETF RFC 768。
- UPnP：见 ISO/IEC 29341。
- 支持 MPEG-2 TS/IP 流媒体传输协议栈操作系统软件要求。

9.3 系统升级

机顶盒应支持操作系统的全部升级和局部升级，且操作系统升级后，不影响原有终端管理客户端和 IPTV 客户端的继续正常使用。机顶盒应支持通过网络方式进行局域网或远程升级：

- 局域网升级：机顶盒应支持在局域网内部，通过电脑或专用工具对机顶盒进行升级；
- 远程升级：机顶盒支持通过与终端管理平台的连接实现开机自动升级或由终端管理平台控制的强制升级。

无论机顶盒采用以上何种方式进行系统软件版本的升级，在软件升级过程中均应在图形界面以图文及动态进度条的方式显示升级进度状态的变化，其中应至少包含几个状态：版本检查、软件下载、软件安装等。

9.4 系统开机

9.4.1 开机方式

智能机顶盒必须支持以下开机方式：

- 断电开机：关机状态下，通过机顶盒面板电源按键进行开机；
- 带电开机：待机状态下，通过遥控器上电源键进行开机。

以上描述的“关机”及“待机”状态是指下述要求：

- 关机状态：机顶盒处于断电状态，无法用遥控器开机，所有状态灯熄灭；
- 待机状态：通过遥控器电源键关闭正在使用的机顶盒，机顶盒仍处于带电状态，此时，网络断开，可用遥控器开机，机顶盒电源灯处于点亮状态。

9.4.2 图像信号

智能机顶盒在开机过程中的图像信号应满足以下要求：

- 在断电及带电开机过程中，应保证图像信号无闪烁、无跳动、无黑屏；
- 开机时应能展现预先加载在机顶盒本地的开机画面。

同时要求，机顶盒应支持通过远程配置或远程升级实现终端开机页面的调整。

9.4.3 开机过程

智能机顶盒开机后立即(<5s)在视频输出端输出指定的画面；智能机顶盒断电开机过程总时间应小于 120s，并以图文结合动态进度条的方式进行提示，开机默认进入 IPTV 首页。

机顶盒开机过程中的状态及相应提示信息应至少包括：

- 操作系统加载：操作系统加载指 IPTV 机顶盒在开机后加载软件系统为后续网络连接、业务接入认证等做好准备；
- 网络连接：网络连接指机顶盒通过 DHCP、PPPoE 和静态 IP 三种方式中的一种获取机顶盒连接网络的 IP 地址；
- 业务认证：业务认证指机顶盒通过预先配置的认证地址、账号及密码连接终端管理平台进行机顶盒及业务合法性认证的状态。

9.5 系统关机

9.5.1 关机方式

机顶盒应支持以下关机方式:

- 断电关机

开机状态下,通过机顶盒面板电源按键进行关机,机顶盒进入断电状态,所有状态指示灯熄灭,且无法通过遥控器电源键进行开机。

- 带电关机

也称为“待机”,通过遥控器电源键关闭机顶盒,使机顶盒进入待机状态,电源等处于点亮状态,可通过遥控器再次开机。

9.5.2 图像信号

机顶盒在关机过程中的图像信号无特殊要求。

9.5.3 关机过程

机顶盒应在 2s 内完成从开机状态到断电关机或待机状态的切换。当机顶盒通过遥控器进入关机或待机状态时,应断开所有网络连接。

9.6 操作要求

智能机顶盒在业务使用过程中应满足以下要求:

——在任意状态下,按下遥控器“本地/应用”按键,进入智能机顶盒首页(桌面),智能机顶盒首页要求另行规定。通过上下左右、确定按键选择各个应用;

——在任意状态下,按下遥控器上的“首页”按键,进入各应用首页;

——机顶盒接受遥控器操作,从当前菜单页面切换到下一个菜单页面完整显示时间应小于 1s;

——机顶盒接受遥控器操作,在菜单页面内的焦点移动时间应小于 0.5s;

——机顶盒支持软键盘输入操作,输入法采用指定方式。

9.7 配置要求

9.7.1 配置要求的基本内容

机顶盒应在出厂时进行终端本身参数的设置,并支持通过本地管理菜单、局域网连接的配置页面或工具、终端管理平台远程管理等多种方式进行机顶盒本身相关参数的配置及查看。

9.7.2 本地配置

机顶盒必须支持以下的本地配置和查看,即可在开机状态下的任何时候通过遥控器“系统/配置”键关闭当前播放的音视频内容,并将主界面跳转至本地配置界面。允许通过遥控器输入预先设置的登陆密码进入本地配置页面进行以下参数的配置与查看:

- 基本设置

——连接方式:可查看并修改网络连接方式为“有线连接”或“无线连接”;

——接入方式:可查看并修改是否启用 IPV6、可支持 3 种网络连接方式:

1) PPPoE:当选择此种方式时,要求支持通过遥控器输入 PPPoE 用户名及密码;

2) DHCP;

3) 静态 IP:当选择此种方式时,支持通过遥控器输入静态 IP、子网掩码、默认网关及 DNS 服务器(主备)。

● 系统信息

- 设备信息：可查看该机顶盒厂家名称、设备型号等；
- 版本信息：可查看该机顶盒软件版本、硬件版本等；
- 网络信息：可查看该机顶盒 MAC、IP、子网掩码、默认网关、DNS 服务器、无线信号状态及强度等；
- 服务器信息：可查看终端管理平台地址、NPT 地址等。

● 高级设置

主要包括与机顶盒操作系统等相关信息的查看及设置，如语言文字、输出制式、所属时区、输出画面显示调整等；

- 输出画面显示调整：支持用户根据实际显示情况，调整水平内缩和垂直内缩，直到调整到最适当的内缩比例。

● 恢复默认设置

默认设置是指在机顶盒出厂时完成的对于机顶盒部分参数的预先配置。通过“恢复默认设置”即可将机顶盒已配置参数恢复为出厂时的配置。

9.7.3 局域网配置

机顶盒应支持在局域网内部，通过电脑或专用工具以 Web 或图形客户端的方式对机顶盒进行配置。机顶盒对于通过局域网进行配置的方式仍应支持密码保护，且可配置及查看的参数不应少于本地配置中列出的参数。

9.7.4 远程配置

机顶盒应支持通过终端管理平台实现对于机顶盒的远程管理，其中涉及的详细参数及配置流程可后续根据要求升级支持。

10 应用层

10.1 应用层的内容

智能机顶盒应用软件是指在系统软件基础上，安装的各种应用软件。应用软件主要包括 IPTV 应用、本地媒体应用等应用软件。

10.2 IPTV 应用

10.2.1 IPTV 应用的内容

IPTV 功能主要包括电视直播、即时时移、点播和电视回看等功能，其中涉及与 IPTV 业务平台的接口请见 YD/T 1696.1、YD/T 1696.2、YD/T 1696.3、YD/T 1696.4 的要求。

10.2.2 页面要求

支持 IPTV 页面的正常显示。对于用户界面的显示，要具体见 YD/T 1696.3。

10.2.3 电视直播

用户可以通过智能机顶盒根据频道直接选择并收看电视节目，系统侧向选择该直播频道的全部用户同时推送相同的音视频流，播放既定的内容，为用户提供电视节目。针对直播电视，机顶盒至少支持如下功能：

- 用户可以通过智能机顶盒由 EPG 页面链接或直接输入频道号的方式进入直播频道；
- 在直播观看过程中，通过遥控器可进行多个直播频道间的切换，可随时离开当前直播频道。

10.2.4 即时时移

用户可以通过智能机顶盒对实时播放的视频直播频道进行短暂的暂停、倒退和快进等操作。针对即时时移功能，机顶盒至少支持如下功能：

- 用户可以通过遥控器控制智能机顶盒在直播与即时时移互相切换（即时时移暂停）；
- 用户可以在即时时移中进行 2X、4X、8X、16X、32X，64X（可选）倍速的快进快退、定位播放等操作；
- 用户可在即时时移中随时通过遥控器操作切换回当前正在播放的直播频道或直接退出即时时移。

10.2.5 点播

用户可以通过智能机顶盒对在平台侧存储的音视频内容进行播放、暂停、快进快退、重放等操作。针对点播功能，机顶盒至少支持如下功能：

- 用户可以通过遥控器控制智能机顶盒在 EPG 中选择点播节目进行播放；
- 用户可在点播节目播放中进行 2X、4X、8X、16X、32X，64X（可选）倍速的快进快退、定位播放等操作；
- 用户可在点播节目播放中随时通过遥控器操作退出当前正在播放的点播节目。

10.2.6 电视回看

用户可以通过智能机顶盒对在平台侧的指定时间内直播过的电视节目进行播放、暂停、快进快退、重放等操作。针对电视回看功能，机顶盒至少支持如下功能：

- 用户可以通过遥控器控制智能机顶盒在 EPG 中选择回看节目进行播放；
- 用户可以在电视回看播放中进行 2X、4X、8X、16X、32X，64X（可选）倍速的快进快退、定位播放等操作；
- 用户可在电视回看功能中随时通过遥控器操作退出当前正在播放的电视回看节目。

10.2.7 图像质量

智能机顶盒在 IPTV 直播、点播、即时时移、电视回看等视频业务的使用过程中，采用主观评价的方式对于智能机顶盒的视频图像质量进行评估，并应达到以下要求：

- 视频内容正常播放时无马赛克、无明显跳动、停滞感，且无唇音不同步现象；
- 视频内容在快进、快退、暂停恢复、定位播放等情况下，图像帧显示清晰、无马赛克。

10.2.8 声音质量

智能机顶盒在直播、点播、即时时移、电视回看等视频相关基本业务的使用过程中，采用主观评价的方式对于智能机顶盒的声音质量进行评估，并应达到以下要求：

- 音频或节目伴音正常播放时，声音流畅，无停顿；
- 直播频道的音量大小与相同情况下的电视节目音量大小一致；
- 机顶盒开机初始音量应在最大音量的中间值附近，并应保证直播和点播内容音量大小一致。

10.3 媒体共享

要求智能机顶盒支持以下媒体共享功能：

- 数字媒体接收（DMR）：可以通过有线或无线家庭网络从其他终端设备接收数字媒体流；
- 数字媒体播放（DMP）：可以播放通过有线或无线家庭网络从其他终端设备接收数字媒体流。

——对于以上功能目前比较厂家的是 DLNA Architectures and Protocols 的要求。

10.4 本地媒体

本地媒体功能是指对本地存储设备内的视频、音频、图片等媒体文件进行浏览观看。智能机顶盒支持本地媒体的管理和播放功能，具体要求如下：

——视频文件播放：支持对于单个视频文件的单独播放或多个视频文件的顺序播放，在播放过程中支持视频文件的屏播放，并可在播放过程中对于进行拖动进度条的快进快退、定位播放、退出等操作。

——音频文件播放：支持对于单个音频文件的单独播放或多个音频文件的顺序播放、随机播放、循环播放等。可支持在音乐播放过程中的图片播放功能，并允许用户配置播放的图片列表。

——图片文件播放：支持单个 1MKB 大小图片文件的小尺寸预览及全屏播放，图片浏览中可支持背景音乐播放，并允许用户配置选择背景音乐的播放列表。在图片播放过程中，可支持多个图片文件的顺序播放、循环播放，并可设置自动播放的时间间隔。至少支持缩放、上升、擦除、下降、展开、淡入淡出等图片切换效果，并允许用户在多个图片的播放过程中进行暂停、恢复、退出等操作。

——外挂字幕：外挂字幕是指字幕文件是独立于视频文件的，播放时使用字幕插件调用字幕，叠加到视频当中。机顶盒至少支持 SRT 和 SUB 两种格式外挂字幕的显示，字幕字库支持 GBK、ISO8859，并支持简体中文及英语显示的显示，其中简体中文字体应支持黑体和宋体。字幕的显示应保持与视音频的同步，且允许用户在节目观看中进行多字幕键的切换。

——应用软件安装：禁止机顶盒通过 USB 接口将本地存储的文件下载及安装到机顶盒上。

10.5 终端管理

10.5.1 终端管理的内容

终端管理相关功能要求请见 YD/T 1696.5，如需支持基于 OTP 的终端安全认证，参见附录 A.3。

10.5.2 运行要求

作为智能机顶盒的基础管理功能，终端管理模块应满足以下技术要求：

——优先启动：终端管理模块应保证在系统启动堆栈中进行注册，以保证在用户本地界面最终完成启动并面向用户提供服务时，终端管理模块已经完成启动并可正常实现相关业务要求；

——后台运行：终端管理模块应采用系统服务的方式进行注册，以保证在智能机顶盒运行过程中始终运行；

——安全保护：终端管理模块应作为软件系统关键进程受到运行保护，无法被用户主动关闭。

10.5.3 兼容性

兼容性要求终端管理应用在不同芯片上可以正常运行，主要包括两个方面：

——跨芯片方案：终端管理功能应该基于统一的芯片接口的前提下实现以上业务管理功能，即要求与终端芯片自身的 API 无关；

——跨系统软件版本：应在智能操作系统无根本性的改变的情况下(如系统自身 API 发生重大变化)，能够在不同的系统软件版本上运行，并要求新版本实现对于旧有软件系统的前向兼容。

10.5.4 协作性

终端管理模块作为智能机顶盒的关键管理功能模块，应采用安全的系统接口与各应用间进行通信、协作及管理功能，即要求终端管理模块能够实现相关业务认证数据、终端信息、应用安装运行的关键信息及状态管理。

10.6 其他应用

要求智能机顶盒支持加载应用，即通过后续下载、安装和升级支持的应用软件。

附录 A (资料性附录)

基于硬件 OTP 的终端安全保护方案

A.1 CPU

对于智能机顶盒操作系统、应用安装等的权限进行控制，机顶盒 CPU 应符合如图 A.1 所示的安全功能模块的要求。

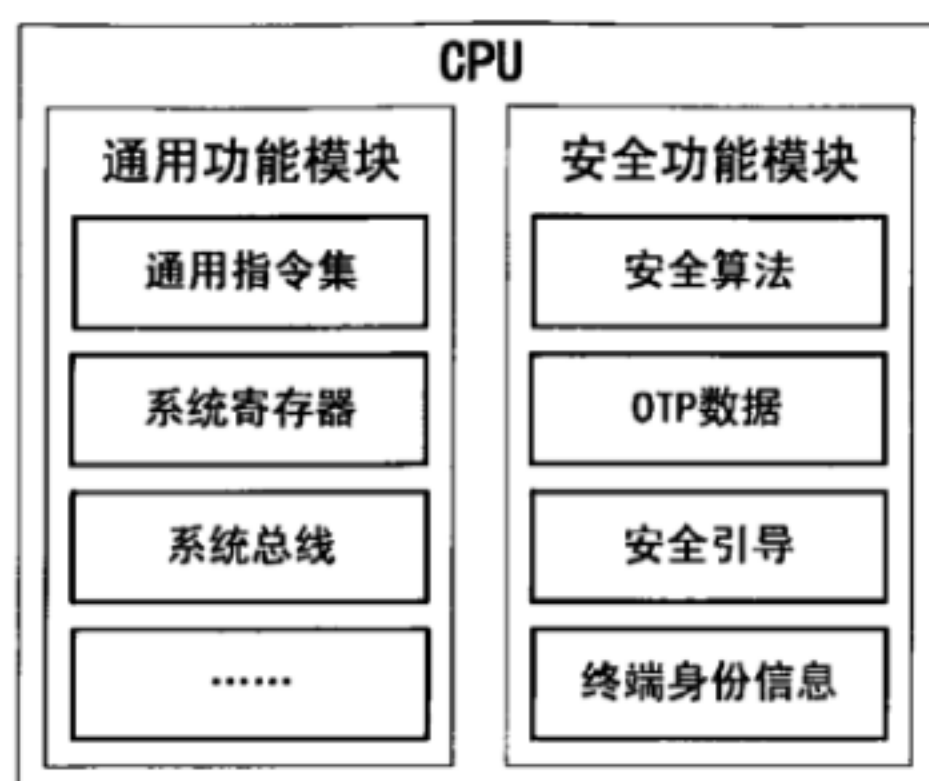


图 A.1 CPU 架构要求

A.1.1 通用功能模块

CPU 的一般功能，执行 CPU 指令系统，运行内存中的指令序列，执行操作系统软件与应用软件。

A.1.2 安全功能模块

安全功能模块用于存放用户以及普通域的代码不能直接可接触的数据，支持安全算法，存放确保应用所需的 OTP 数据，并执行安全引导过程，为操作系统及应用软件提供根本的安全保障。运行于 CPU 内部，有独立与外部总线的存储空间用于运行安全处理程序与存储中间结果。安全算法涉及的数据以及中间结果均对外部 CPU 所执行的外部指令不可见。

安全相关关键数据主要包括对称算法密钥，非对称算法公钥，用于认证的单向 hash 的基本初始序列。这些数据在机顶盒上的数据存储方式必须为下述方式之一：

- 以明文存储在 CPU 外部指令无法读取的 OTP 区域。
- 以密文存储在外部的 Flash 某区域之中，但需要对该区域进行数字签名，并在使用这些数据之前进行签名验证合法性。

安全功能模块的详细要求应满足以下描述：

● 片内引导程序

CPU 在开始运行外部程序之前需要有软件检测过程，通过对将要执行的 CPU 指令序列进行合法性检测，在确保将要执行软件是合法软件后才能开始执行该部分软件。如果确认将要执行的软件不具备合法性，则必须停止执行软件，并通过硬件方式进行状态指示。

● 安全算法引擎

安全算法引擎是指用于数据加解密、数字签名与验证的相关算法的计算引擎。CPU 的安全算法必须支持对称加密算法、非对称加密算法以及单向 hash 算法三类。表 A.1 列出了可用的安全算法列表。

表 A.1 可用安全算法列表

算法类型	算法名称
对称加密算法	AES-128(CBC, EBC, CTS, CTR)
	DES
	3DES
非对称加密算法	RSA-1024
	RSA-2048
hash 算法	SHA256
	SHA1
	HMAC-SHA1
	CBC-MAC

● OTP 数据

OTP 数据空间支持具备安全的批量录入方法，OTP 数据可分为可读取数据与不可读取数据两部分，其中可读取数据可通过安全模块的读取方法进行读取操作，主要包括：

——SN：芯片唯一标识序列号；

——RSA 公钥。

不可读取数据则不能通过 CPU 指令以及任何其他的基于软件或硬件的 CPU 调试手段获取，主要包括：

——IN：芯片内部唯一序列号；

——运营商标识；

——ChipID：芯片类型编号；

——对称加密算法密钥。

注：签名验证的数据均由厂商提供的专用工具在软件包制作过程中产生，并随原数据相同的渠道安装到机顶盒。

● 终端身份信息

机顶盒 SN 是一串存放在 OTP 中的终端唯一标识，长度 24 字节，由图 A.2 所示的几个部分组成。

厂商代码 4 字节	终端型号 4 字节	产品批次 8 字节	产品序号 8 字节
-----------	-----------	-----------	-----------

图 A.2 终端序列号

机顶盒 IN 是普通域不可读的內部序列号，长度 24 字节，具有唯一性，由图 A.3 所示的几部分组成。

厂商代码 4 字节	芯片批次 8 字节	芯片序号 12 字节
-----------	-----------	------------

图 A.3 终端内部序列号

对于终端身份信息的认证可采用如图 A.4 的流程。

终端管理程序与内核驱动程序均运行在终端软件系统的普通域，实现平台的身份认证协议。在这个身份认证过程中终端必须在内核提供安全域访问的驱动程序，并提供应用调用 API。内核驱动程序将终端管理程序 API 的相应请求发送到 CPU 安全域，由其返回对应的结果。

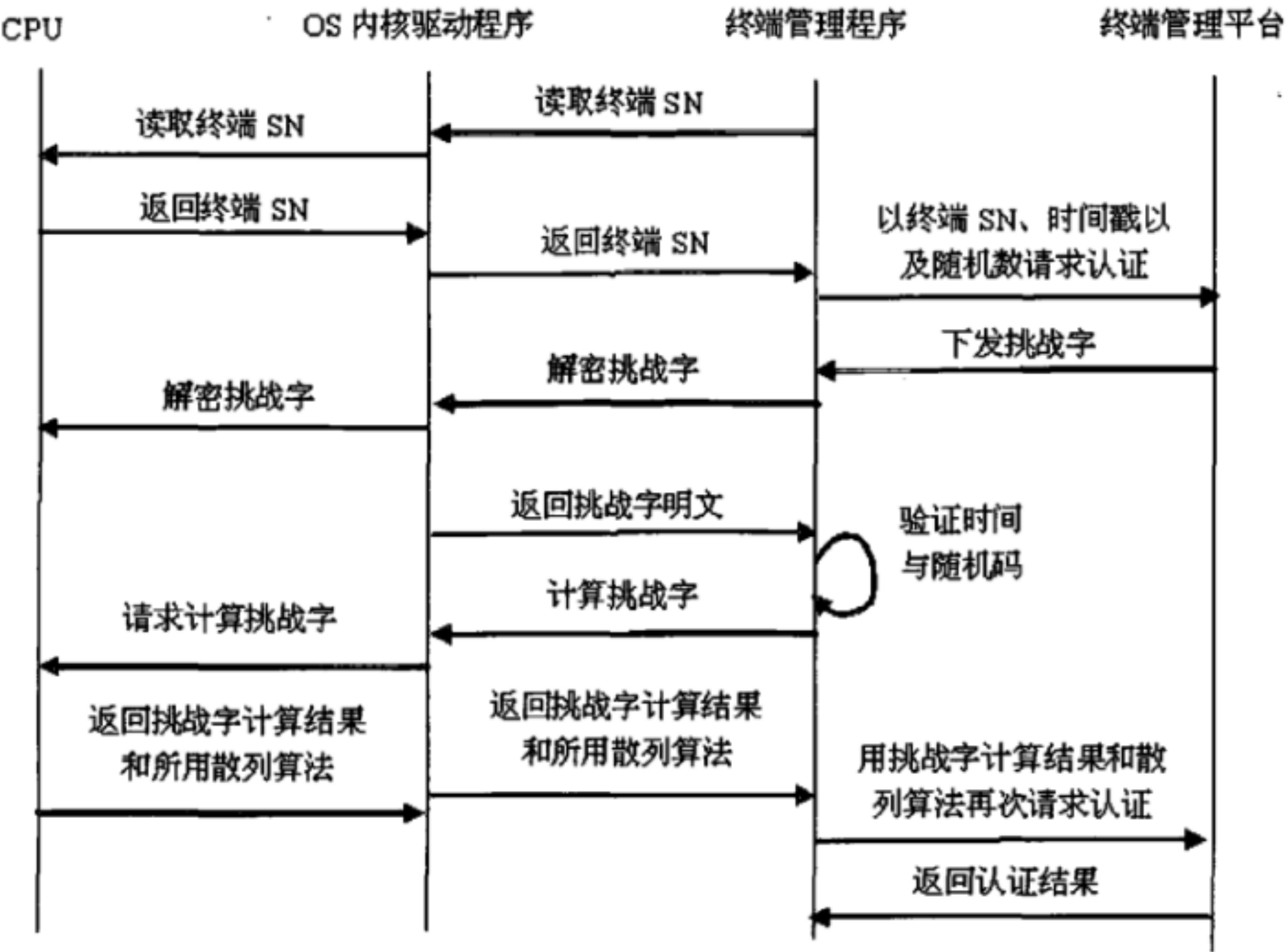


图 A.4 终端身份认证流程

在以上流程中，挑战字由平台对如图 A.5 所示的挑战字原文数据用 RSA1024 私钥加密产生。

运营商标识 4 字节	终端时间戳 14 字节	终端随机数 16 字节	平台时间戳 14 字节	平台随机数 16 字节
------------	-------------	-------------	-------------	-------------

图 A.5 挑战字原文数据结构

图 A.5 所示的挑战字原文共 64 字节，其中运营商标识符 4 字节，时间戳采用数字表示的时间形式，具体为 `yyyymmddhhmmss`，即 4 字节数字年，月日时分秒各 2 字节。终端随机数与终端时间戳由终端产生并在请求认证消息中发送到平台。

终端管理请求 CPU 安全域必须将挑战字解密，获得挑战字原文，并对运营商标识、终端时间戳、终端随机数进行对比验证，然后才能进行挑战字的计算。

挑战字验证过程如下：

挑战字返回结果由安全域计算。终端管理程序将挑战字原文中的运营商代码、平台时间戳与平台随机数发送给 CPU；CPU 安全域在收到挑战字计算请求并验证运营商标识正确后，用 OTP 中保存的 SN、ChipID、IN，加上平台时间戳、平台随机数，用散列算法计算散列值作为挑战字计算的返回值。散列算法输入的定义如图 A.6 所示。

SN: 24 字节	ChipID: 4 字节	IN: 24 字节	平台时间戳: 14 字节	平台随机数: 16 字节
-----------	--------------	-----------	--------------	--------------

图 A.6 散列算法输入定义

A.2 操作系统

为支持OTP安全芯片智能操作系统需支持与芯片OTP相关的硬件信息、操作系统、应用加密等相关的驱动

A.2.1 系统引导

支持权限管理功能的智能机顶盒的启动过程必须符合图 A.7 所示的基本流程。

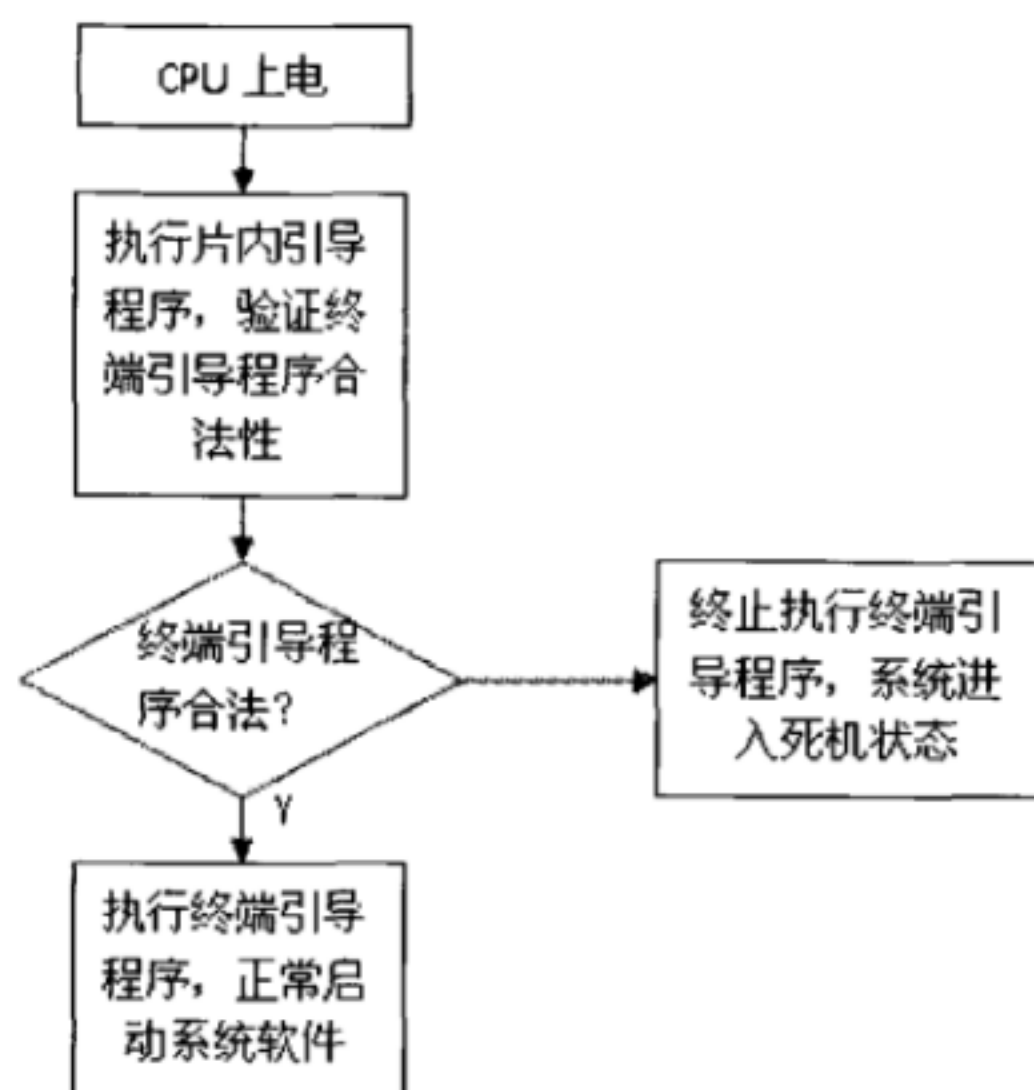


图 A.7 支持权限管理功能的智能机顶盒的系统验证过程

CPU 对引导程序的验证可采用安全、有效的验证算法, 如基于 SHA256+RSA2048 的数字签名验证, 或基于 AES128 加密的代码加密方法。用于验证的密钥必须确保安全性, 如必须使用存放的 OTP 区域的密钥, 如果使用存放在 flash 中的密钥, 则必须使用安全有效的加密与签名验证机制确保密钥的安全。

终端启动过程中必须对引导程序的签名验证采用全覆盖签名验证, 且必须具备对验证算法关键数据的生成与管理工具。

终端的引导程序通过合法性验证后, 它必须对后续引导过程执行的代码进行合法性验证。根据系统状态, 终端引导程序可能执行的代码包括系统内核或系统恢复程序, 其执行过程必须符合如图 A.8 所示基本流程。

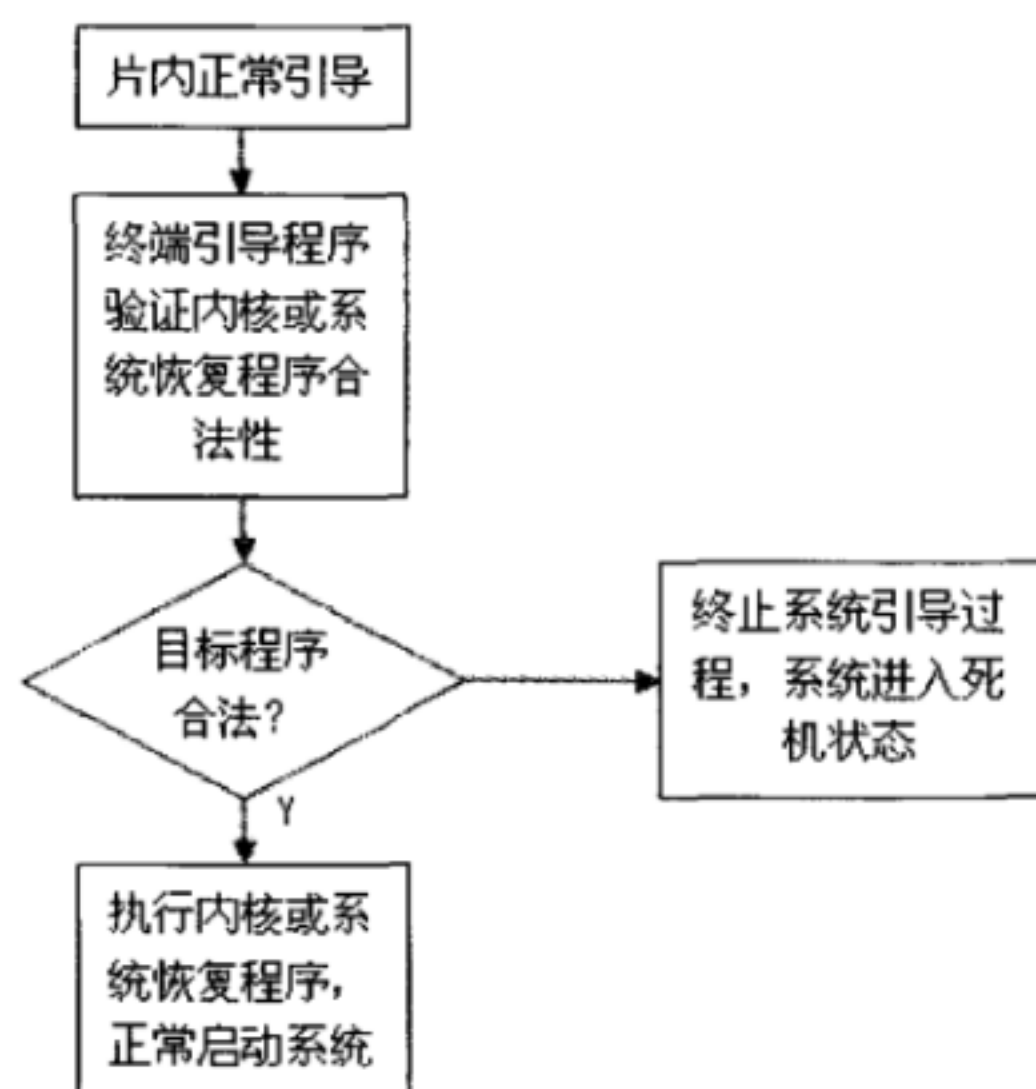


图 A.8 支持权限管理功能的智能机顶盒系统引导过程

终端引导程序对内核或系统恢复程序的合法性验证必须采用安全、有效的验证算法, 且必须提供对

验证算法关键数据的生成与管理工具。

上述验证算法可以是如基于 SHA256+RSA2048 的数字签名验证，或基于 AES128 加密的代码加密方法。用于验证的密钥必须确保安全性，如必须使用存放的 OTP 区域的密钥，如果使用存放在 flash 中的密钥，则必须使用安全有效的加密与签名验证机制确保密钥的安全。

对内核或系统恢复程序的签名验证必须采用全覆盖签名验证。

当内核被引导后，内核需要以文件系统方式或其他方式加载系统数据区中的数据。内核在加载系统数据区之前必须随机的对系统数据区的数据进行合法性验证，该验证过程可以是整个数据区验证，为了提升系统启动速度，也可以对系统数据区采用随机抽样的片区数据验证方式进行合法性验证。

系统恢复程序必须支持 OTA 方式的系统升级或恢复过程，形成可用的系统内核区、系统数据区与用户数据区。在系统升级或系统恢复过程中，系统恢复程序必须对将要用于系统升级或恢复的所有数据采用与引导程序相同的合法性验证方法进行验证。

A.2.2 权限管理 API

对于 CPU 中部署有安全芯片的智能机顶盒来说，其操作系统应支持以下的接口定义及调用流程：

● API 调用软件结构

API 调用软件结构如图 A.9 所示。

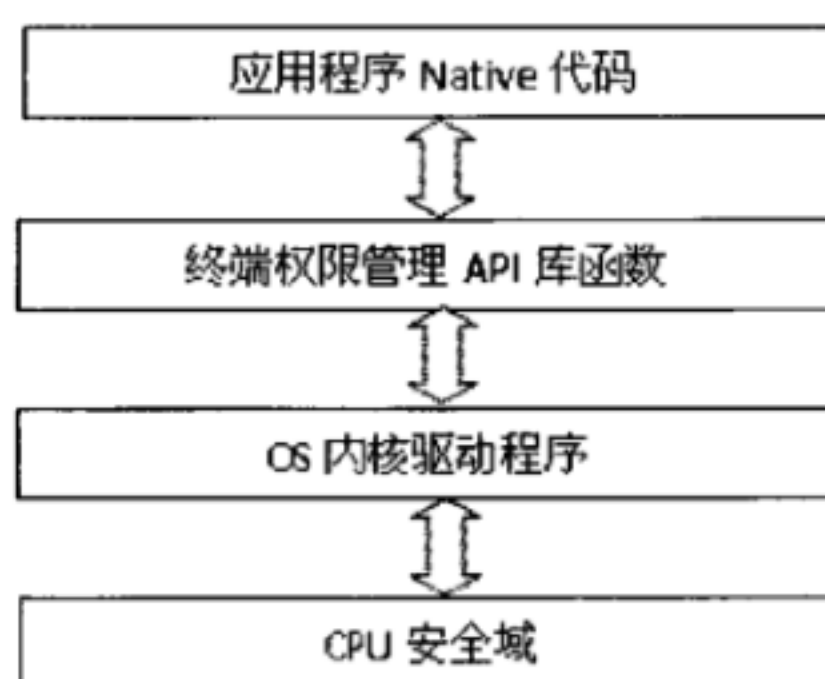


图 A.9 系统结构调用示意图

图 A.9 中指出了终端必须提供 C 函数 API 供应用的 Native 代码调用，该 API 函数通过 CPU 安全域的内核区程序直接访问 CPU 安全域的计算功能。

CPU 安全域通过终端安全 API 提供给应用程序的能力包括：

- 终端 SN 访问；
- 终端认证接口访问；
- 安全算法计算访问；
- 终端安全 API 定义。

智能机顶盒应在 Linux Kernel 的 Security_Driver 中提供本标准中定义的 API 功能，但为保证终端安全 API 的高安全性，各终端需自行命名安全 API 的名称，在本标准中定义的 API 命名仅供参考。

● 挑战字计算

`void challenge(char *dat, int *length, char *hash);`

dat 为输入数据与返回值数据指针，length 为输入数据长与返回数据长度度指针，hash 为安全域所采用的散列算法，均为调用者分配；其中 hash 返回值定义为：0：SHA1；1：SHA256；2：HMAC-SHA1；

3: CBC-MAC。

● 读取 SN

int readSN(char *dat);

——dat 为返回值数据指针，由调用者分配，函数返回数据长度。

● 数字签名验证

int check_digitsign(char *dat, int dat_length, char *sign, int sign_length);

对输入的数据 dat 与签名 sign 进行验证，返回验证结果，验证不成功返回 0，验证成功返回 1。

——dat: 需要签名确认的原始数据指针；

——dat_length: 上述数据长度；

——sign: 需要确认的签名数据；

sign_length: 上述数据长度。

● 解密函数

void decipher(int encryption_type, char *dat, int *length);

——encryption_type: 加密函数类型；

——dat: 加密数据缓冲，输出为明文数据；

——length: 数据长度。

A.2.3 系统升级

需要注意的是，如需基于 CPU 安全芯片进行终端权限管理的智能机顶盒应满足以下软件版本生成、系统升级流程

● 版本生成

● 系统软件生成流程如图 A.10 所示。

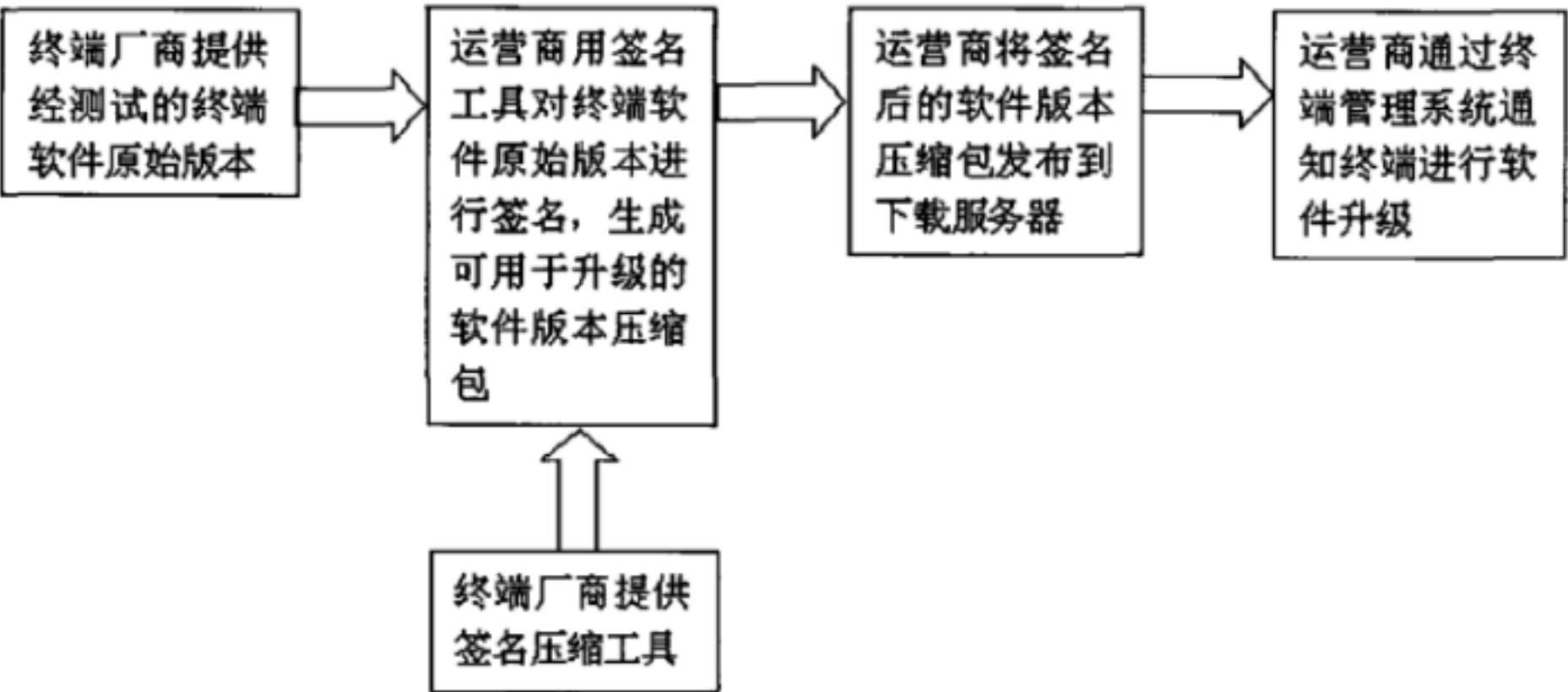


图 A.10 系统软件生成流程

软件准备过程中的签名压缩工具由终端厂商统一提供，该工具生成可由 Recovery 进行签名验证的系统升级压缩包。生成的系统升级压缩包可包含 Recovery 程序、kernel 映像、rootfs 映像的任意组合集，并包含相应的版本信息。

● 升级流程

系统软件升级基本流程如图 A.11 所示。

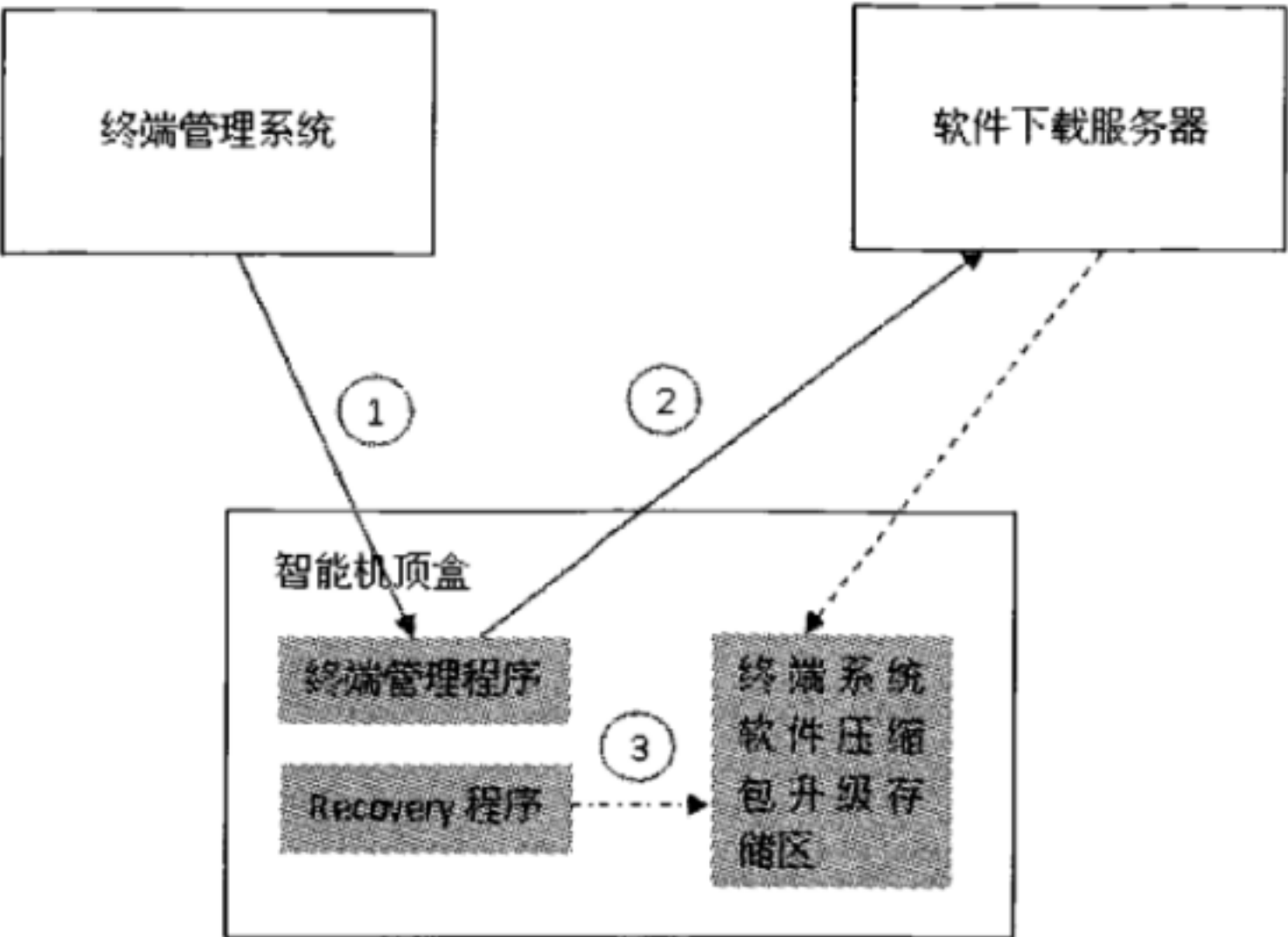


图 A.11 软件升级基本流程

如图A.11所示，智能机顶盒终端软件系统升级涉及终端管理系统、软件下载服务器以及智能机顶盒。软件升级的总体流程如下：

- 1) 当智能机顶盒的系统软件有升级版本时，终端管理系统通过智能机顶盒管理接口通知终端管理程序，并将软件的下载服务器URL下发终端管理程序。
- 2) 终端管理程序从软件下载服务器下将终端的系统软件下载到终端FLASH闪存中的终端系统软件升级存储区，并设置终端软件升级标志，然后重启终端。
- 3) 当终端重启后，终端引导程序检测到终端软件升级标志，启动终端的Recovery程序，由该程序对终端软件升级存储区中的软件进行签名检验，签名检验通过后执行软件升级操作，并清除升级标志。

注：Recovery 程序在进行系统升级时必须对相应部分进行签名验证，对签名错误的软件包不进行升级，确保升级后系统不会因为签名不正确不能正常启动。同时，系统自动升级过程中必须对用户进行相应提示。

A.3 终端管理客户端

基于 YD/T 1696.5 中定义的终端管理功能要求，为支持采用权限管理的软件升级、终端身份认证、应用保护等功能，并具有系统 ROOT 权限，其详细的业务功能需求如下：

- 终端信息安全：能够安全地保护终端上的厂商、硬件型号、终端串号等相关信息，并应保证无法通过修改软件的手段对于终端的信息进行修改。同时，还应保证仅可通过终端侧提供的手段提供对于终端基本信息的读取(不包括写入)；
- 系统保护：对于基于智能操作系统的终端，由于其系统软件的开放性，因此要求未经认证的系统软件无法在智能机顶盒上进行安装
- 终端身份验证：主要根据终端安全信息提供的数据，用于验证该终端是否为己注册的合法终端；
- 应用保护：应对于在该软件系统上通过应用商城进行安装的应用软件提供高级别的安全保护，安装在智能机顶盒上的应用软件无法直接从智能机顶盒上复制并无法直接在未经认证的终端上进行安装使用；
- 软件升级：应能够实现智能机顶盒的软件系统的安全升级，只有通过认证的软件操作系统才可在智能机顶盒上进行安装、升级。

附录 B

(资料性附录)

智能机顶盒IPTV业务功能实现API

IPTV_MediaProcessor (IPTV媒体处理库) 主要是接收TS裸流, 并通过不同的播放状态通过硬件解码器进行音视频的解码及输出等工作。

此部分功能主要用于实现与芯片相关的音视频输出、音量控制、音视频编解码等硬件相关的功能, 当IPTV_MediaProcessor的相关方法被IPTV_MediaControl (IPTV媒体控制) 调用时, 在相应方法中应根据其实际的播放、显示状态对于相应的音视频输出、编解码器等的输出及缓存进行状态的更新。

B.1 基类定义

```
class IPTV_MediaProcessor{
public:
    IPTV_MediaProcessor (){}
    virtual ~MediaProcessor(){}
public:
    //取得播放模式
    virtual int  GetPlayMode()=0;
    //显示窗口
    virtual int  SetVideoWindow(int x,int y,int width,int height)=0;
    //x 显示视频
    virtual int  VideoShow(void)=0;
    //隐藏视频
    virtual int  VideoHide(void)=0;
    //初始化视频参数
    virtual void InitVideo(PVIDEO_PARA_T pVideoPara)=0;
    //初始化音频参数
    virtual void InitAudio(PAUDIO_PARA_T pAudioPara)=0;
    //开始播放
    virtual bool StartPlay()=0;
    //暂停
    virtual bool Pause()=0;
    //继续播放
    virtual bool Resume()=0;
    //快进快退
    virtual bool Fast()=0;
    //停止快进快退
    virtual bool StopFast()=0;
    //停止
    virtual bool Stop()=0;
    //定位
    virtual bool Seek()=0;
```

```

//设定音量
virtual bool SetVolume(int volume)=0;
//获取音量
virtual int GetVolume()=0;
//设定视频显示比例
virtual bool SetRatio(int nRatio)=0;
//获取当前声道
virtual int GetAudioBalance()=0;
//设置声道
virtual bool SetAudioBalance(int nAudioBalance)=0;
//获取视频分辨率
virtual void GetVideoPixels(int& width, int& height)=0;
//是否由软件拉伸, 如果由硬件拉伸, 请返回 false
virtual bool IsSoftFit()=0;
//设置 EPG 大小, 标清固定 640*530, 高清是 1280*720, 在高清平台中有些页面还是 640*530, 会随时在这两种分
//分辨率中切换, 所以要做到根据不同分辨率来进行拉伸
virtual void SetEPGSize(int w, int h);
};

//获取 IPTV_MediaProcessor 派生类的实例对象。在 GetMediaProcessor() 这个接口的实现中, 需要创建一个
//IPTV_MediaProcessor 派生类的实例, 然后返回这个实例的指针
IPTV_MediaProcessor* GetMediaProcessor();

```

B.2 SetVideoWindow

函数: int SetVideoWindow(int x,int y,int width,int height)
参数描述: x: 视频窗口的左偏移 (像素)。 y: 视频窗口在上偏移 (像素)。 width: 视频窗口宽度 (像素)。 height: 视频窗口的高度 (像素)
返回值: 0-表示成功。如果不成功则显示不正常
说明: 在屏幕的指定区域显示视频, 如果是软拉伸, 会根据从 GetVideoPixels 接口中取得的参数进行转换成当前显示系统的绝对显示位置, 如果是硬件拉伸, 则是 EPG 中的原始值 (标清时全屏是 640*530, 高清时是 1280*720, 窗口模式时就是 EPG 原有的值)

B.3 GetPlayMode

函数: int GetPlayMode()
参数描述: 无
返回值: 1
说明: 取得播放模式, 直接返回 1。 保留用于扩展

B.4 VideoShow

函数: int VideoShow(void)
参数描述: 无
返回值: 0-表示成功。如果不成功则显示不正常
说明: 显示视频

B.5 VideoHide

函数: int VideoHide(void)
参数描述: 无
返回值: 0-表示成功。如果不成功则显示不正常
说明: 隐藏视频, 当调用 Stop 后希望保留最后一帧的显示, 而调用该方法时再清除最后一帧, 如果 Stop 后不保留最后一帧, 那么换台的时候将会是黑屏

B.6 InitVideo

函数: void virtual InitVideo(PVIDEO_PARA_T pVideoPara)
参数描述: PVIDEO_PARA_T pVideoPara: typedef struct{ unsigned short pid;//pid int nVideoWidth;//视频宽度 int nVideoHeight;//视频高度 int nFrameRate;//帧率 vformat_t vFmt;//视频格式 IPTV 的为 VFORMAT_H264, 参见附录 A unsigned long cFmt;//编码格式 IPTV 的为 CODEC_TAG_H264 }VIDEO_PARA_T, *PVIDEO_PARA_T;
返回值: 无
说明: 初始化视频参数

B.7 InitAudio

函数: void virtual InitAudio(PAUDIO_PARA_T pAudioPara)
参数描述: PAUDIO_PARA_T pAudioPara: typedef struct{ unsigned short pid;//pid int nChannels;//声道数 int nSampleRate;//采样率 aformat_t aFmt;//音频格式 IPTV 的为 AFORMAT_MPEG, 参见附录 A int nExtraSize; unsigned char* pExtraData; }AUDIO_PARA_T, *PAUDIO_PARA_T;
返回值: 无
说明: 初始化音频参数

B.8 StartPlay

函数: virtual bool StartPlay()
参数描述: 无
返回值: 0-表示成功。如果不成功则无法播放。
说明: 开始播放, 调用 StartPlay 之后, 会开始调用 WriteData 写入数据

B.9 WriteData

函数: virtual int WriteData(unsigned char* pBuffer, unsigned int nSize)
参数描述: pBuffer: ts 流数据地址 nSize: 写入字节数
返回值: 成功返回传入的 nSize, 失败返回-1, 如果返回-1, 10ms 之后会再次写入相同的数据
说明: 把 ts 流数据传入硬件解码模块

B.10 Pause

函数: bool Pause()
参数描述: 无
返回值: 0-表示成功
说明: 通知硬件解码模块应用层暂停播放

B.11 Resume

函数: bool Resume()
参数描述: 无
返回值: 0-表示成功
说明: 通知硬件解码模块应用层继续播放

B.12 Fast

函数: bool Fast()
参数描述: 无
返回值: 0-表示成功
说明: 通知硬件解码模块应用层快进快退, 调用 Fast 后收到的 TS 流只有视频没有音频, 不需要进行同步, 收到一帧显示一帧, 清除未处理数据

B.13 StopFast

函数: bool StopFast()
参数描述: 无
返回值: 0-表示成功
说明: 通知硬件解码模块应用层停止快进快退, 之后收到的数据是正常播放时的数据, 需要重新音视同步。清除未处理数据

B.14 Stop

函数: bool Stop()
参数描述: 无
返回值: 0-表示成功
说明: 通知硬件解码模块应用层停止播放

B.15 Seek

函数: bool Seek()
参数描述: 无
返回值: 成功返回 true, 失败返回 false
说明: 清除未处理数据, 重新同步音视频。该接口在定位时及组播转时移时会调用

B.16 SetVolume

函数: bool SetVolume(int volume)
参数描述: 设置声音
返回值: 成功返回 true, 失败返回 false
说明: 设定播放器音量 (0~100), 暂未使用

B.17 GetVolume

函数: int GetVolume()
参数描述: 无
返回值: 当前播放器音量
说明: 暂未使用

B.18 SetRatio

函数: bool SetRatio(int nRatio)
参数描述: nRatio
返回值: 成功返回 true, 失败返回 false
说明: 设定视频显示比例。暂未使用

B.19 GetAudioBalance

函数: int GetAudioBalance()
参数描述: 无
返回值: 当前使用的声道: 1:左声道, 2:右声道, 3:双声道
说明: 获取当前声道

B.20 SetAudioBalance

函数: bool SetAudioBalance(int nAudioBalance)
参数描述: nAudioBalance
返回值: 成功返回 true, 失败返回 false
说明: 设置声道。1:左声道, 2:右声道, 3:双声道

B.21 GetVideoPixels

函数: void GetVideoPixels(int& width, int& height)
参数描述:
width: 输出参数, 视频系统宽度 (像素)
height: 输出参数, 视频系统高度 (像素)
返回值: 无
说明: 获取视频系统显示分辨率, 不是当前影片的分辨率

B.22 IsSoftFit

函数: bool IsSoftFit()
参数描述: 无
返回值: 返回 true, EPG 由上层进行拉伸, 返回 false, EPG 由硬件拉伸
说明: 是否由软件拉伸, 如果由硬件拉伸, 返回 false

B.23 SetEPGSize

函数: void SetEPGSize(int w, int h)
参数描述:
w: 宽度
h: 高度
返回值: 无
说明: 设置 EPG 大小, 标清固定 640*530, 高清是 1280*720, 在高清平台中有些页面还是 640*530, 会随时在这两种分辨率中切换, 所以要做到根据不同分辨率来进行拉伸。当 IsSoftFit 返回 true 时, 该接口不用实现

B.24 SetSurface

函数: void SetSurface(Surface* pSurface)
参数描述:
pSurface: 宽度
返回值: 无
说明: 本函数用于 Android 4.0, 用于将 surface 传给播放器, 从而显示视频画面。Surface 是 Android 图形机制的结构, 其定义详见 Android 头文件

中华人民共和国
通信行业标准
IPTV 机顶盒技术要求
智能型

YD/T 2726-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路1号邮电出版大厦
邮政编码: 100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2015年12月第1版
印张: 2.5 2015年12月北京第1次印刷
字数: 64千字

15115·532

定价: 30元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492