ICS 33.160
M 70/79

团　体　标　准

T/CVIA-33-2014 代替

CVIA/ZNDS05—2014

智能电视应用商店技术规范

2014- 01-10 发布　　2014- 01-10 实施

中国电子视像行业协会　　发 布

目　　次

前言 III
1　概述 1
2　定义和缩略语 2
2.1　定义 2
2.2　缩略语 2
3　应用商店功能描述 2
3.1　商店管理后台功能描述 2
3.1.1　应用管理： 3
3.1.1.1　应用信息管理 3
3.1.1.2　应用上线 3
3.1.1.3　应用下线 3
3.1.1.4　入库归档 4
3.1.1.5　应用检索 4
3.1.1.6　应用黑名单 4
3.1.1.7　应用删除 4
3.1.1.8　应用状态流转控制 4
3.1.1.9　应用交易管理 5
3.2　终端及用户管理 5
3.2.1　运营支撑模块
3.3　接口服务及资源分发 6
3.3.1　WebService 业务接口服务器 6
3.3.2　应用资源下载服务器 6
3.4　客户端功能描述 6
3.4.1　客户端升级 6
3.4.2　客户端 UI 及交互 7
3.4.3　终端用户登录 7
3.4.3.1　自动注册登录 7
3.4.3.2　人为注册登录（可选） 8
3.4.4　应用的分类及呈现 8
3.4.4.1　应用浏览 8
3.4.4.2　应用详细信息 8
3.4.5　应用搜索 8
3.4.6　应用下载管理功能 9
3.4.6.1　存储路径管理 9
3.4.6.2　下载操作 9
3.4.7　应用购买 9

3.4.8 应用管理功能 9
3.4.8.1 已安装应用 9
3.4.8.2 应用布局管理（可选） 10
3.4.8.3 应用的同步及升级 10
3.4.8.4 应用运行 10
3.4.8.5 应用的卸载 10
3.4.9 应用收藏夹（可选） 10
3.4.10 用户评价（可选） 10
3.4.11 用户信息（可选） 10
3.4.11.1 定制推送业务支持（可选） 10
4 应用商店系统技术规范 10
4.1 商店平台规范 10
4.1.1 硬件要求 11
4.1.1.1 主机系统 11
4.1.1.2 存储设备 11
4.1.1.3 备份设备 12
4.1.1.4 核心网络设备 12
4.1.1.5 防火墙 12
4.1.1.6 其他要求 13
4.1.2 软件要求 13
4.1.2.1 系统软件要求 13
4.1.2.2 操作系统 13
4.1.2.3 数据库 13
4.1.3 系统要求 14
4.1.3.1 系统可靠性 14
4.1.3.2 信息安全 15
4.1.3.3 扩展性要求 16
4.1.4 接口服务及资源下载 16
4.2 客户端规范 17
4.2.1 客户端集成环境 17
4.2.1.1 操作系统环境 17
4.2.1.2 硬件环境： 17
4.2.1.3 分辨率： 17
4.2.1.4 安装包要求 17
4.2.1.5 动态运行 RSS 内存 17
4.2.2 可管可控(可选择配置) 17
4.2.2.1 第三方应用禁止安装 17
4.2.2.2 应用加解密 17
4.2.2.3 应用内升级拦截 17
4.2.3 客户端与系统模块的集成： 17
4.2.4 异常处理 18

前　　言

本规范为推进智能电视健康发展，降低各厂商应用商店的不规范建设，增强智能电视产品的兼容性，根据智能电视的产业化现状而制定，是智能电视标准体系的一部分。

本规范规定智能电视应用商店的功能要求，主要是终端、后台以及运营支撑的技术规范，本规范可用于指导智能电视应用商店的相关研发及部署。

本规范由中国电子视像行业协会提出并归口。

本规范起草单位：中国电子视像行业协会、广州欢网科技有限责任公司、青岛海尔电子有限公司、青岛海信电器股份有限公司、TCL 集团股份有限公司、深圳创维-RGB 电子有限公司、四川长虹电器股份有限公司、康佳集团股份有限公司、深圳市中彩联科技有限公司等单位共同起草。(排名不分先后)

本规范主要起草人：白为民、郝亚斌、冯晓曦、刘秀云、姜钧凯、杨海波、王志国、李晓榕、李微、郭建伟、李大勤、董波、余潘虎、纪萍、严帅领、邓文科、张新法、田卫平、吴伟、张曼华(排名不分先后)

智能电视应用商店技术规范

1　概述

1.1　本规范规定了终端与应用之间在平台、客户端协议上的互通要求。

1.2　本规范规定了以宽带为主要接入方式的集团、个人、家庭智能电视用户提供应用商店功能。

1.3　本规范建议每种型号的智能电视机采用唯一商店。

1.4　本商店可以由厂商按标准分别进行建设，不同厂商及其智能电视运营平台，需按照统一的方式进行组建应用商店。

1.5　本商店要求提供基本的 QOS 管理能力;提供支付计费功能;具有系统级容灾备份等功能。

1.6　应用程序商店是通过网络下载用户喜爱的应用程序，为终端用户提供资讯、娱乐、生活、教育等丰富多彩的软件服务。包括应用的收集、管理以及对于终端的接口服务等业务能力的支撑。

1.7　逻辑结构图

应用商店整体业务涵盖的各主要实体，通过下图说明：

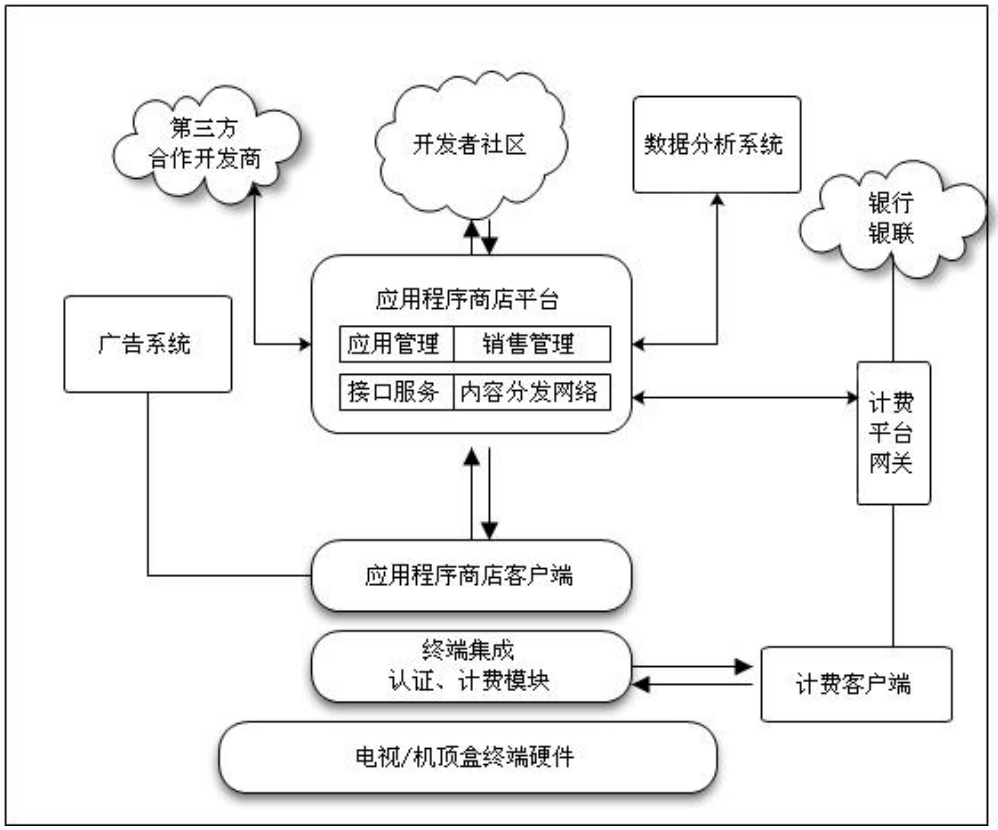


图 1：应用商店整体示意图

2 定义和缩略语

2.1 定义

智能电视应用商店是预装到智能电视机、用于利用各方资源实现功能扩展、具有端到端服务质量保障，满足智能电视终端应用下载、安装、管理等需求的服务体系。

2.2 缩略语

下列缩略语适用于本规范：

AS	Application Server	应用服务器
API	Application Program Interface	应用程序编程接口
DRM	Digital Rights Management	数字版权管理

EPG	Electronic Program Guide	电子节目指南
HDTV	High Definition Television	高分辨率电视
ID	Identity	身份标识号码
ISC	IP multimedia Subsystem Service Control	IMS 业务控制
LAN	Local Area Network	局域网
NTP	Network Time Protocol	网络时间协议
OS	Operating System	操作系统
SDTV	Standard Definition Television	标准分辨率电视
SP	Service Provider	服务内容提供者
TMS	Terminal Management System	终端管理系统
URI	Uniform Resource Identifier	统一资源标识
URL	Uniform Resource Locator	统一资源定位
APS	App Store Server	应用商店平台
APC	App Store Client	应用商店客户端
商品		应用商店内发布的应用

3 应用商店功能描述

3.1 商店管理后台功能描述

应用商店的管理后台，作为整个商店的服务提供核心平台，从功能上需要具备以下的主要功能模块：

3.1.1 应用管理：

主要实现应用开发商的管理及应用引入，包括应用管理、合作管理、开发支持、运营审核等功能。

在应用引入的基础上，实现应用商店业务的管理，包括应用管理、用户管理、订购管理、应用版权控制、下载分发、触发计费、货架管理、热卖促销、终端适配、主动营销、统计分析报表等功能。

应用商店的应用类型主要包括软件、教育、游戏、资讯等。

3.1.1.1 应用信息管理

应用信息中包含商品的基本信息、关键信息、应用分类等。

——基本信息

包括应用名称、应用图片、应用描述、应用关键字、应用价格、应用分类。

——关键信息

包括应用的关联产品信息、归属开发商信息（开发者信息）、应用适配版本等。

——应用分类

应用商店管理员可以添加、删除应用分类，可以修改应用和应用类的对应关系；该应用分类可以和应用分类一致，例如游戏、娱乐等，系统可支持多级子目录的分类，列出大类别中的子类及应用列表，点击子类可继续分类别查找，用户可以根据应用分类目录逐层查找需要的应用。

删除某种应用分类时要求该应用类的所有应用已经下线。

只有应用商店管理员才能进行应用分类的建立和更改。

3.1.1.2 应用上线

应用商店首先对接入的应用进行审批，审批通过后进行上线处理，正式发布。

审批内容包括应用的元数据信息，应用版本的描述、应用的价格（虚拟币）等等。

内容审核模块支持以下功能：

——应用审批人员可以方便地对通过、未通过、待通过审查的应用进行浏览、状态标注，对不能通过审查的应用填写原因，对审核的内容添加文字批注，然后反馈给相应的负责人；

——可以对用户进行分角色定义，灵活对不同的角色授予权限；

——可以灵活的对审批流程进行定义；

——可以对审批流程进行追踪，同时可以进行方便的通知。

3.1.1.3 应用下线

应用下线可能包括以下几种情况：

——开发商提出下线申请

——应用实体文件损坏

——应用包含不合法因素

根据下线需求，相关管理员对该应用进行下线处理，将门户页面上的展示信息屏蔽，并根据下线的原因进一步对应用实体文件进行相应的处理：续约、要求开发商重新上传等。

3.1.1.4 入库归档

入库归档是对在应用商店发布过的已经下线的应用的相关历史信息数据的保存和管理，记录下线原因和相关操作日志，可作为数据分析、后期查询等需要的依据。

3.1.1.5 应用检索

应用商店管理员可以根据开发者/开发商、发布时间属性、销售量、评价分等级、应用状态等信息查找应用信息，可以根据时间段、应用编码、开发者/开发商、版权保护属性、应用状态、销售量、评价分等级等条件排序输出，管理员可对检索到的应用信息进行查看、上线、下线、删除等操作。

3.1.1.6 应用黑名单

应用的元数据和实体中包含有不合法因素的情况下，管理员可强制将已经上线的应用加入黑名单。加入黑名单的应用状态为下线状态。

应用商店客户端定时更新黑名单信息，对已经安装了黑名单中应用的用户，系统将阻止运行该应用，并提示用户进行该应用的卸载。

3.1.1.7 应用删除

应用删除是在应用实体中含有不合法因素或是开发者终止在应用商店销售该应用时，管理员可以对商品的元数据和实体信息进行删除清理。

只有已下线的应用才能进行删除操作。

3.1.1.8 应用状态流转控制

应用商店的应用状态包括待审批状态，审批未通过状态，上线状态，下架状态四个状态。

应用的状态流转控制参见下图：

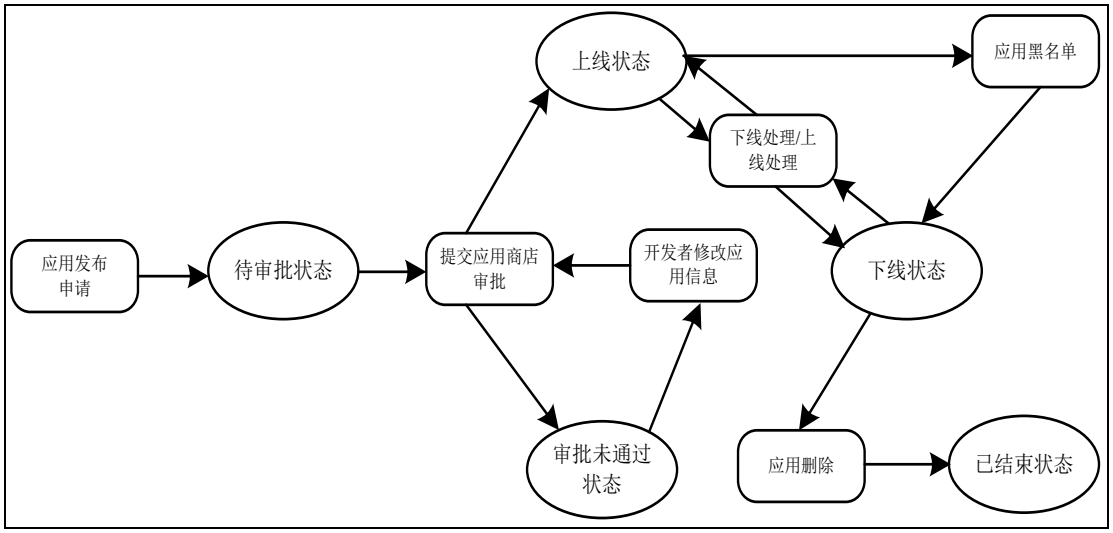


图 2 ：应用状态流转图

通过审核流程后才能正式上线。应用商店管理员可以根据需要对应用进行上线或是下线处理。

对于已上线的应用，管理员可强制将该应用加入黑名单中。加入黑名单的应用状态变更为下线状态。

应用下线后，应用商店管理员可根据需要对应用进行删除处理，应用删除后，应用进入已结束状态。

3.1.1.9 应用交易管理

当一个用户成功下载一个应用时，系统生成一条交易记录，交易记录包含不限于交易编号、用户标识、终端标识、应用名称、应用版本编号、交易时间、应用价格（虚拟币）、交易状态、应用归属开发商/开发者编号。

系统可根据需要，按应用、按用户信息、按应用版本、按交易时间段、按开发商/开发者信息查询输出交易信息。

3.2 终端及用户管理

a） 用户登陆

应用商店展现时获取终端唯一标识信息，如用户为第一次登陆应用商店，则系统默认为该用户进行注册。

b） 应用购买

用户按照应用商店计费规则进行应用购买。

c） 用户退出/登出

系统提供退出/登出功能。

d) 推送策略管理

可对用户进行推送或不推送某些应用或功能的管理。

e) 收藏夹

收藏夹用于保存用户感兴趣的应用。

用户对收藏夹里的应用可以进行删除、分组、加入购物车、购买等操作。

f) 个人资料管理

个人资料包括基本资料信息、用户属性信息，用户在登陆状态时可对个人资料的信息进行填写或修改。

g) 浏览历史记录管理

浏览历史记录用于保存用户最近浏览的应用。

h) 评价管理

评价是用户对该应用的运行、界面等各方面的综合满意度进行评价。

应用商店管理员不能修改用户做出的评价。

3.2.1 运营支撑模块包括运维支持、用户注册管理、用户信息管理、统计报表、结算管理、客服支撑和定制推送管理等功能。

3.3 接口服务及资源分发

3.3.1 WebService 业务接口服务器

商店平台通过 Web Service 接入服务器向终端提供各种服务接口。

3.3.2 应用资源下载服务器

商店平台通过 CDN 分发用户需要下载安装的资源，在终端需要下载具体的应用时，可以提供快速的下载服务。

下载服务器需要有鉴权的功能，防止非法终端对于应用的下载。

3.4 客户端功能描述

3.4.1 客户端升级

客户端应支持定制终端预置安装，下载安装等方式安装。

客户端支持 HTTP 下载方式的升级。在新版本软件发布时，客户端应能获取到该信息并提示用户进行升级。客户端升级结束后，原用户个性化数据和设置仍然保留。

当客户端软件需要进行升级时，客户端支持两种升级方式：

强制升级：当客户端连接网络时，如果客户端检测到有新的软件版本，会自动进行下载然后升级软件。

可选升级：当客户端连接网络时，如果客户端检测到有新的软件版本，会通知用户是否进行下载然后升级软件。

支持增量升级功能，当客户端中非核心模块升级时，可以只升级此更新模块，不需要重新下载、安装全新的客户端。

所有升级不成功的情况下，都能保证用户正常启动旧客户端重新登录。

3.4.2 客户端 UI 及交互

应用商店客户端所有的功能设计都是以为用户提供良好的用户操作感受、用户业务体验为关键，以推动应用的销售为目的，完成用户从应用接触、应用购买到应用使用等一系列业务流程。

应用商店客户端必须支持遥控器、鼠标、触摸方式的混杂交互场景，确保在以上交互时业务逻辑合理正常。

客户端主要业务功能围绕下图展开：

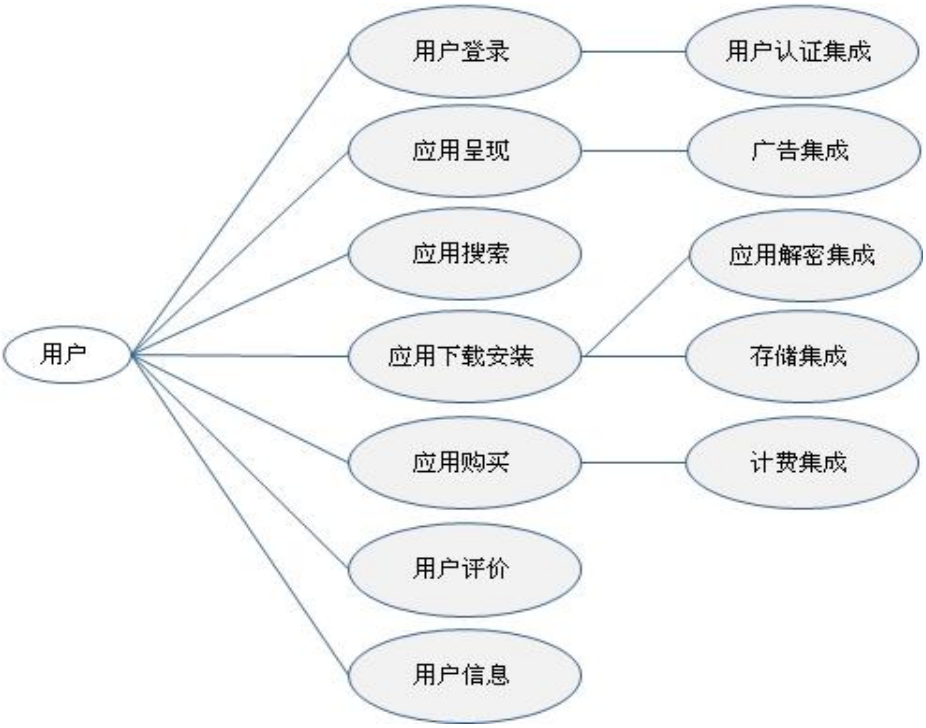


图 3 ：客户端功能主要用例示意图

3.4.3 终端用户登录

3.4.3.1 自动注册登录

对于 TV 应用商店客户端，系统可采用自动注册登录方式。用户运行应用商店客户端，客户端获取用户硬件唯一标识信息，通过该信息进行登录操作。应用商店获取该硬件标识信息并返回客户端用户相关信息。

如果用户通过客户端第一次访问应用商店系统，则系统默认为该用户进行注册操作。

3.4.3.2 人为注册登录（可选）

对于应用商店客户端，用户可根据自己偏好进行注册，并通过登录操作关联其应用商店的属性。

3.4.4 应用的分类及呈现

客户端可以获取应用分类和信息，客户端和服务器之间采用 XML 文件格式进行数据交互。客户端支持文字、图片的综合呈现。以适合客户端界面的效果展现分类和应用信息。以下分类的具体名称，可以自行定义，本规范体现的分类名称仅仅是作为索引。

3.4.4.1 应用浏览

提供各种不同的浏览视图，以便用户快速的定位应用。

——分类浏览

- 客户端可展示应用的分类，用户可以通过分类查找应用。
- 客户端可支持多级子目录的分类，列出大类别中的子类及应用列表，点击子类可继续分类别查找，用户可以根据应用分类目录逐层查找需要的应用。

3.4.4.2 应用详细信息

通过获取应用详细信息在客户端界面进行浏览。

——应用名称

——应用图标

——价格（可选）

——应用截图

——应用介绍

——应用类型（可选）

——开发者（可选）

——发布时间（可选）

——相关评论（可选）

——评分（可选）

——应用的其他属性（可选）

3.4.5 应用搜索

客户端提供对所有应用的搜索功能。

3.4.6 应用下载管理功能

用户能够通过客户端将已购买的应用及应用的升级包、客户端的升级包等通过下载管理功能下载到电视设备本地。

3.4.6.1 存储路径管理

如果选择的存储空间已满或没有发现存储设备时，客户端必须提示用户。

3.4.6.2 下载操作

——即时下载

用户可以通过客户端进行即时下载操作，当选择即时下载时，此应用应进入下载队列，优先级最高。相同优先级的下载任务按时间先后排列。客户端在下载过程中应能够正确显示下载信息页面，包括下载队列中各应用的应用名称、下载完成百分比、下载建立时间、下载用时等，且相关信息应实时变化。

——断点续传（可选）

如果正在下载队列中的文件没有下载完成，客户端需要提供断点续传功能。该功能不需要用户的干预。

——下载提示

- 正在下载
- 暂停下载
- 取消下载
- 下载完成
- 下载安装

3.4.7 应用购买

用户通过客户端浏览应用，并选择感兴趣的应用进行购买。

3.4.8 应用管理功能

3.4.8.1 已安装应用

——可执行操作

- 运行
- 卸载
- 升级（可选）

3.4.8.2 应用布局管理（可选）

对已安装的应用，用户可根据需要自行排列顺序和布局。

可以在电视终端设备启动智能功能后，将已下载的应用，自动分类到相关文件夹或功能区。

3.4.8.3 应用的同步及升级

客户端可从服务器端取得已下载应用列表，当发现用户安装的应用存在更新版本时，应用商店可通知用户升级，但不支持未通过审核的升级。

3.4.8.4 应用运行

对于已安装应用，可执行启动操作，并上报运行日志。

3.4.8.5 应用的卸载

对于已下载安装的应用，用户可选择做卸载操作。

3.4.9 应用收藏夹（可选）

收藏夹用于保存用户感兴趣的应用，可迅速定位查看应用详情。

3.4.10 用户评价（可选）

客户端能够提供对应用的评价等用户互动功能。

3.4.11 用户信息（可选）

可通过客户端软件，查询用户个人基本资料。其中硬件信息不可修改。

3.4.11.1 定制推送业务支持（可选）

客户端能够提供定制推送业务支持。

用户在浏览应用、下载应用时，客户端播放指定的定制推送内容。定制推送内容可以包括文本、图片、视频。定制推送内容通过后台管理系统添加和管理，客户端在恰当的时间（登录时或闲时）从服务器动态获取。

应用商店应支持与定制推送平台接口，应用商店、客户端的定制推送内容可由定制推送平台统一管理。

4 应用商店系统技术规范

4.1 商店平台规范

应用商店后台管理功能，需要提供浏览器界面管理，兼容主流的浏览器 IE8、Chrome 等，在技术实现上需要具备高可靠性，通过集群方式实现系统可扩展性。在关键数据上实现数据的异地备份。

4.1.1 硬件要求

应用商店系统设计和建设时必须从网络平台、服务器平台、数据库平台和应用软件等方面进行全面考虑，通过热备份、事故监控和网络安全保密等多种技术措施，提供较强的管理机制和控制手段，保证系统运行和业务数据的安全和一致性，以保证系统的正常运行、业务的正常开展。

4.1.1.1 主机系统

对于关键性业务应用主机要求如下：

——要求采用主流服务器或小型机，支持多处理器，采用 64 位处理器；

——主要模块要求组成双机或多机高可用群集系统；

——多机群集系统中的每个主机都应同时处于工作状态，并根据配置的情况运行相同或者不同的应用（或应用模块），以保证主机资源的充分利用；

——在计算机硬件、操作系统、存储系统及应用系统业务进程出现故障时，能迅速响应并进行应用的切换；

——主机的处理能力要求满足所有业务应用和一定用户规模的需求，而且需考虑全部系统的开销及应用切换时性能余量。系统设计时应考虑 15%的性能冗余；

——内存容量的配置要考虑到主机正常运行状态下的内存利用率不应大于 85%，保证系统在业务高峰时仍具有较强的抗冲击能力；

——主机应支持 500Mb/s 等高速连接接入应用商店平台核心局域网；

——主机的硬盘、网络接口、网络连接及电源均应考虑足够的冗余；

——支持电源、I/O 设备、存储设备的热插拔；

——主机系统设备应具有适当的扩充能力，包括 CPU 的扩充、内存容量的扩充及 I/O 能力的扩充等，并可支持 CPU 模块的升级和群集内节点数的平滑扩充。

4.1.1.2 存储设备

存储设备主要指磁盘阵列，实现应用商店平台数据的联机存储。

——磁盘阵列设备要求有很高的安全可靠性；

——磁盘阵列设备应可与多种厂家的主机系统相连；

——磁盘阵列应能配合多机高可用群集系统的需要；

——磁盘阵列支持标准接口，可提供多通道、双电源及冗余风扇；

——磁盘阵列设备应具有较强的平滑扩充能力，包括系统存储容量的扩充及 I/O 能力的扩充等；

——磁盘阵列应支持先进的存储、备份方式。

4.1.1.3 备份设备

应用商店平台中的备份设备指大容量的磁带库或光盘库等，主要用于应用商店平台数据的脱机备份。

——备份设备要求有良好的安全可靠性；

——备份设备可与多种厂家的主机系统相连；

——磁带库要求支持标准接口。大型的磁带库设备要求提供冗余的数据接口和机械手设备；

——备份设备应具有较强的平滑扩充能力，包括系统设备容量的扩充及 I/O 能力的扩充等。

4.1.1.4 核心网络设备

核心网络设备应满足下述要求：

——网络采用 TCP/IP 协议，主干网络采用高速网络；

——路由器产品必须符合通用的国际工业化标准；

——核心交换机采用热旁路路由器协议 HSRP 协议，实现双机互为备份；

——核心交换机提供三层交换能力，同时提供等路径路由，实现负载均衡；

——接入交换机采用 STP 协议，同时连接到两台核心交换机上，避免单点失败；

——核心局域网划分 VLAN，由核心交换机实现网段间路由；

——核心交换机及中心路由应采用高可靠的设备，具备背板冗余功能，系统板、关键 I/O 板、电源、风扇等考虑冗余，并可热插拔；省中心节点、地市节点要求双路由器配置，并保证路由器的互相热切换备份；

——主干网络设备的配置端口总数应能满足应用和用户规模的要求，并保留约 10%的余量，同时应保证适当的扩展能力；

——支持 SNMP 和 SNMPv2 协议。

4.1.1.5 防火墙

防火墙可以采用主机加防火墙软件或专用的防火墙设备，应满足下列要求：

——支持动态和静态的内部网与外部网之间的地址转换、映射；

——能有效地实现内部网到外部网的单向访问控制，可以禁止外部网对内部网的访问；

——能侦测、过滤或跟踪非法访问企图，能自动实时告警，并生成相应日志记录；

——能对常用服务的访问权限进行有效控制和管理；能对经过防火墙的网络流量进行统计和管理，并定期生成相应报告文件；

——支持 SNMP 和 SNMPv2 协议。

4.1.1.6 其他要求

设备应能在下列供电变化范围内正常工作：

——直流：－ 40V ～ － 57V。

——交流：～220V ± 10％，50Hz ± 5％，电源波形：正弦波畸变不大于 3%。

4.1.2 软件要求

4.1.2.1 系统软件要求

系统所使用操作系统、数据库、双机软件、备份软件等系统软件，应采用当前业界主流产品，系统软件支持具备磁盘镜像。

4.1.2.2 操作系统

操作系统要求如下：

——关键业务应用主机采用 64 位 UNIX 操作系统，并可兼容以往的 32 位应用系统；

——操作系统支持虚拟内存管理，支持多用户、多任务、多进程和多线程；

——支持完全对称多处理器（SMP）；

——支持群集（cluster）；

——操作系统应至少达到C2级的安全标准；

——操作系统应遵循X/open XPG4, POSIX 1003.1等国际或工业标准；

——提供完整的软件开发环境，包括C，C++编译器等开发工具；

——操作系统应提供图形化的系统管理工具；

——支持在线诊断和软硬件的自动错误记录，在电源故障或其他紧急情况可提供自保护和自恢复；

——支持中文大字符集等相关国家标准。

4.1.2.3 数据库

——支持ANSI/ISO SQL-89、ANSI/ISO SQL-92标准；

——支持中文汉字内码，符合双字节编码；

——支持主流厂商的硬件平台及操作系统平台；

——数据库系统应具有良好的伸缩性；

——支持主流的网络协议（如：TCP/IP、IPX/SPX、NETBIOS及混合协议）；

——具有良好的开放性，支持异种数据库的互访：

- 实现对文件数据和桌面数据库数据的访问；
- 实现对大型异种数据库的访问；
- 能够将原有异种数据库向本数据库无损失移植；
- 实现和高级语言互联的能力；
- 支持XA、ODBC 3.0、X/OpenCLI、JDBC等标准；
- 支持分布式事务及两阶段提交功能。

——具有支持并行操作所需的技术；

——支持网络上同构或异构数据库之间数据的冗余性复制；具有多种复制功能模块；

——支持联机事务处理（OLTP）；支持决策支持的建立，要求能够实现数据的快速装载、高效的并发处理和交互式查询；

——支持C2或以上级安全标准、多级安全控制；

——支持数据库存储加密及相应冗余控制；

——提供Web服务接口模块，对客户端输出协议支持HTTP2.0、SSL等；

——支持联机存储和备份功能；

——应具有强的容错能力、错误恢复能力、错误记录及预警能力；

——数据库、表大小等技术参数可灵活设置，支持对多媒体数据及大数据量处理的技术需求；

——应避免数据库死锁的出现，一旦死锁能够自动解锁；

——开发工具易使用、开发效率高、维护方便；

——支持多种 CASE 工具。

4.1.3 系统要求

本系统是 7×24 小时不间断运行的业务运营平台，其网络、主机、存储设备、系统软件等部分应该具有极高的可靠性；同时为保证系统安全可靠地运行，保守企业和用户秘密，维护企业和用户的合法权益，系统应具备良好的安全策略，安全手段，安全环境及安全管理措施。

4.1.3.1 系统可靠性

——网络

网络设备与网络链路应有冗余备份功能，核心网络设备应采用高可靠的设备；网络设备应保证 7×24 小时不间断运行。

——服务器

关键性服务器应采用高可用性方案。系统应冗余配置，保证系统无单一故障点，发生故障后能够快速切换，保证 7×24 小时不间断运行。

——存储、备份及恢复

存储设备应具有极高的可靠性。系统应有良好的备份手段。系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性。

——应用系统

整个应用系统应能够连续 7×24 小时不间断工作，出现故障应能及时告警，应具有完整的操作权限管理功能和完善的系统安全机制。

应用系统应具备完善的检测功能，确保交互数据的准确性。系统每个环节的检测实行闭环管理，并建立与其它功能模块相对独立的检测系统，校验数据的准确性。应用系统应具备自动或手动恢复措施，以便在发生错误时能够快速地恢复正常运行。应用软件要防止消耗过多的系统资源而使系统崩溃。

要求关键设备之间的切换应能在 2 分钟内完成。

4.1.3.2 信息安全

——物理安全

物理安全是指保护数据业务管理平台中计算机系统、网络设备、信息设施及媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或蓄意犯罪等行为而导致的破坏。物理安全是保障整个平台安全的基础和前提，主要包括如下三个方面：

环境安全：主要指计算机和网络设备所在的机房环境必须保证安全。

设备安全：设备安全主要包括设备的防盗、防毁、防电磁泄漏、防止线路截获、抗电磁干扰、电源保护及防止非法物理访问等。

信息媒体安全：包括媒体数据的安全及媒体本身的安全。

——网络安全

网络系统应支持访问控制、安全检测、攻击监控等一系列安全功能，应提供完整的网络监控、报警和故障处理功能。

网络系统和服务器系统应具有入侵检测的功能，可监控可疑的连接、非法访问等，采取的措施包括实时报警、自动阻断通信连接或执行用户自定义的安全策略。

网络和服务器系统应能定期检查安全漏洞，根据扫描的结果更正网络安全漏洞和系统中的错误配置。

使用加密技术对传输的数据加密。

与其它系统的连接须设置防火墙，并定义完备的安全策略。

——系统安全

系统应具有防病毒能力。防病毒软件应具备全面查杀病毒，查杀病毒准确无误，管理方便，病毒特征码自动更新，安装简单的特点。

系统应具备访问权限的识别和控制功能，提供多级密码口令或使用硬件钥匙等保护措施。对各种管理员必须授予不同级别的管理权限。要保证只有授权的人员或系统可以访问某种功能，获取业务数据，有非法访问或系统安全性受到破坏时必须告警。任何远程登录用户的口令均必须具有有效期，有效期满则自行作废。

系统应提供日志记录功能，以便及时掌握系统安全状态；操作系统应符合 C2 级以上安全标准；提供完整的操作系统监控、报警和故障处理能力；操作系统的配置直接影响系统的安全，应定期对文件、帐户、组、口令的配置检测，以保证操作系统的坚固程度；应定期对可执行程序作完整性检查，以防止

被恶意修改；能够检测操作系统内部是否有黑客程序驻留；能够监控应用程序的运行情况；日志中要求采用错误标识代码准确标识错误点。

数据库应支持 C2 或以上级安全标准、多级安全控制。支持数据库存储加密、数据传输通道加密及相应冗余控制。

系统应提供相应措施保证交易信息、话单信息的完整性/安全性/可靠性。

系统应具有安全审计功能。

——应用软件安全

应用系统的用户管理、权限管理应充分利用操作系统和数据库的安全性；应用软件运行时须有完整的日志记录，必须具有应用监控及调度功能。

4.1.3.3 扩展性要求

应用商店平台应具有灵活性与可扩展性，方便扩展设备容量和提升设备性能。应用商店平台架构应确保系统能平滑升级。系统升级应尽量在不影响正常业务的条件下进行。

4.1.4 接口服务及资源下载

平台通过接口服务器对外提供 Web service 的服务接口，需要支持 http 和 https 的接口方式。部署需要通过集群提供 HA，保证服务的可靠性。

资源下载功能建议通过 CDN 提供。

4.2 客户端规范

4.2.1 客户端集成环境

4.2.1.1 操作系统环境：

——基于本系列标准的操作系统。

4.2.1.2 硬件环境：

——可参考 TV/硬件相关要求和规定。

4.2.1.3 分辨率：

——720P 及以上。

4.2.1.4 安装包要求

——应用商店客户端安装包要求小于 20MB。

4.2.1.5 动态运行 RSS 内存：

——客户端运行时，动态运行 RSS 内存，建议小于 50MB。

4.2.2 可管可控(可选择配置)

4.2.2.1 第三方应用禁止安装

通过系统底层的包管理定制策略，实现对第三方应用的安装管控，以确保非法应用的安装运行。

4.2.2.2 应用加解密

对于应用商店的应用进行特定加密，确保商店下发的应用不被滥用，确保第三方应用不能随意安装。

4.2.2.3 应用内升级拦截

当第三方应用存在应用内升级时，需要进行拦截检测，确认此升级不能绕过商店平台进行。

4.2.3 客户端与系统模块的集成：

4.2.3.1 与用户、设备认证集成

通过与终端厂商的系统集成，确定系统认证的接口；通过系统认证的接口，获取到终端用户、设备的鉴权信息，上报给应用商店平台，由应用商店平台调用认证鉴权模块，确认接口不被非法调用，业务不被非法访问。

4.2.3.2 与计费系统集成

在终端，发生计费业务的时候，调用终端集成环境提供的计费接口，触发计费业务逻辑模块，完成计费环节后，返回应用商店的业务逻辑模块，同时上报平台服务器进行记录及业务处理，完成一次完整的计费流程。

4.2.3.3 与应用安全性集成：

应用商店进行的应用安装，可以和本地安全校验模块进行交互，确保安装的应用是安全可靠不违反底层安全机制的，在异常的安装运行时，上报服务器进行记录，并终止不安全的流程，同时提示用户。

4.2.3.4 与应用安全集成方案：(可选)

为了进一步确保应用的安全性以及可靠性，针对系统安装包 Package Installer，进行二次开发，嵌入定制的加解密模块，确保只有符合加解密标准的应用，方可在终端安装运行，以阻止非法应用及木马的安装所导致终端的业务及安全失控。

4.2.4 异常处理

4.2.4.1 联网异常处理

——登录过程异常

当客户端被打开时，客户端将自动进行登录。如果由于网络原因客户端不能与服务器正常通信，客户端应提示用户网络异常。同时，如在打开客户端时无法获取电视硬件信息，将提示用户设备信息获取异常。

当客户端已经在线使用时，如果由于网络原因客户端不能与服务器正常通信，客户端应在30秒后给出提示，并提供重试、离线与退出的功能。

在订购应用时，如无法获取硬件设备等信息，客户端将提示用户设备信息获取异常，无法进行订购。

——页面列表更新异常

当客户端已经以正常方式（非离线方式）登录后，如果由于网络原因客户端不能及时更新完分类及应用列表信息时，客户端给出提示；当更新时间超时，应提示用户重试或返回上一级目录。

4.2.4.2 存储异常处理

客户端在下载文件之前，应检测存储空间，当空间不足时提醒用户。

4.2.4.3 应用异常处理

当应用异常时，客户端应屏蔽错误或给出友好提示。

本规范由中国电子视像行业协会组织制定和发布，并负责对所有规范的修改、解释。