ICS 33.160
M 70/79

# 团　体　标　准

T/CVIA-34-2014 代替

CVIA/ZNDS06-2014

# 智能电视系统安全技术规范

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 ..... II
1　概述 ..... 1
2　定义和缩略语 ..... 1
2.1　定义 ..... 1
2.2　缩略语 ..... 1
3　安全要求 ..... 1
3.1　安全框架图 ..... 1
3.2　系统加载安全 ..... 2
3.3　内容安全 ..... 2
3.4　应用程序安全 ..... 2
3.4.1　服务端 ..... 3
3.4.2　设备端 ..... 3
3.5　支付安全 ..... 4
3.6　设备认证安全 ..... 4
3.7　API 权限 ..... 4
3.8　越狱和防篡改 ..... 4
3.9　用户数据安全 ..... 4
3.10　数据传输安全 ..... 4

# 前　　言

本规范为推进智能电视产业健康发展，降低各厂商的重复建设，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系统安全要求，可用于指导智能电视多媒体通信终端的研发及部署。

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、四川长虹电器股份有限公司、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、康佳集团股份有限公司、青岛海尔电子有限公司、广州欢网科技有限责任公司、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、邓文科、张新法、李微、郭建伟、李大勤、王志国、李晓榕、姜钧凯、杨海波、董波、余潘虎、纪萍、严帅领、田卫平、吴伟、张曼华（排名不分先后）

# 智能电视系统安全技术规范

## 1 概述

本规范对智能电视的系统安全进行要求，主要包括安全框架、设备认证安全、传输安全、系统加载安全、内容安全、应用安全、支付安全、API权限、越狱和防篡改及用户数据安全。

## 2 定义和缩略语

### 2.1 定义

智能电视系统安全是指对智能电视系统软件的安全保护，对设备、用户以及应用程序进行鉴权及访问控制。防止系统核心内容被非法篡改，并为上层应用提供安全框架和接口。

### 2.2 缩略语

下列缩略语适用于本标准：

| | | |
|---|---|---|
| CAS | Conditional Access System | 条件接收系统 |
| DRM | Digital Rights Management | 数字版权管理 |
| TVOS | Smart TV Operating System | 智能电视操作系统 |
| PKI | Public Key Infrastructure | 公钥基础设施 |

## 3 安全要求

### 3.1 安全框架图

智能电视终端安全架构体系如下所示：

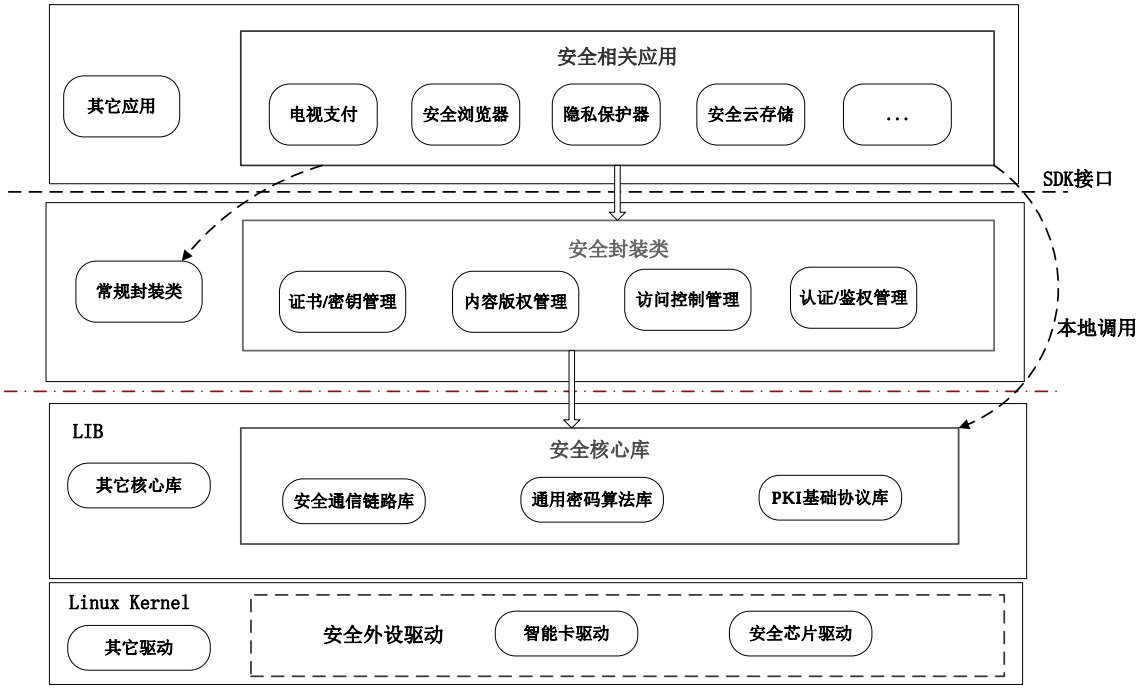



图1：智能电视系统安全框架图

### 3.2 系统加载安全

智能电视操作系统安全机制继承了linux的系统安全机制,为了防止非法用户和软件获取root权限，关闭了获取root权限的途径。为防止系统软件被修改和破坏，需要对系统软件进行签名和校验。

为防止bootloader被篡改，需要对bootloader进行签名校验，而系统启动时会先校验loader，如果loader被篡改，则系统拒绝启动。

### 3.3 内容安全

需提供一个可扩展的DRM框架。这个DRM框架使应用程序可根据内容的相关许可来管理受保护的内容，且支持多种DRM方案。

对于应用程序开发者，DRM框架提供了一个抽象的统一的API，从而简化了对保护内容权限的管理。

### 3.4 应用程序安全

为确保安装在电视上应用程序的安全性，系统应提供一种管理应用程序安装的方式。只有通过供应商审核和签署的应用程序才允许安装到系统中。验证成功后，应用程序可以按标准过程进行安装。

经过签名的应用程序，如果智能终端中没有对应的认证解密模块，也无法安装到智能电视系统中。

基于智能终端厂商的软件二次签名机制如下图所示：

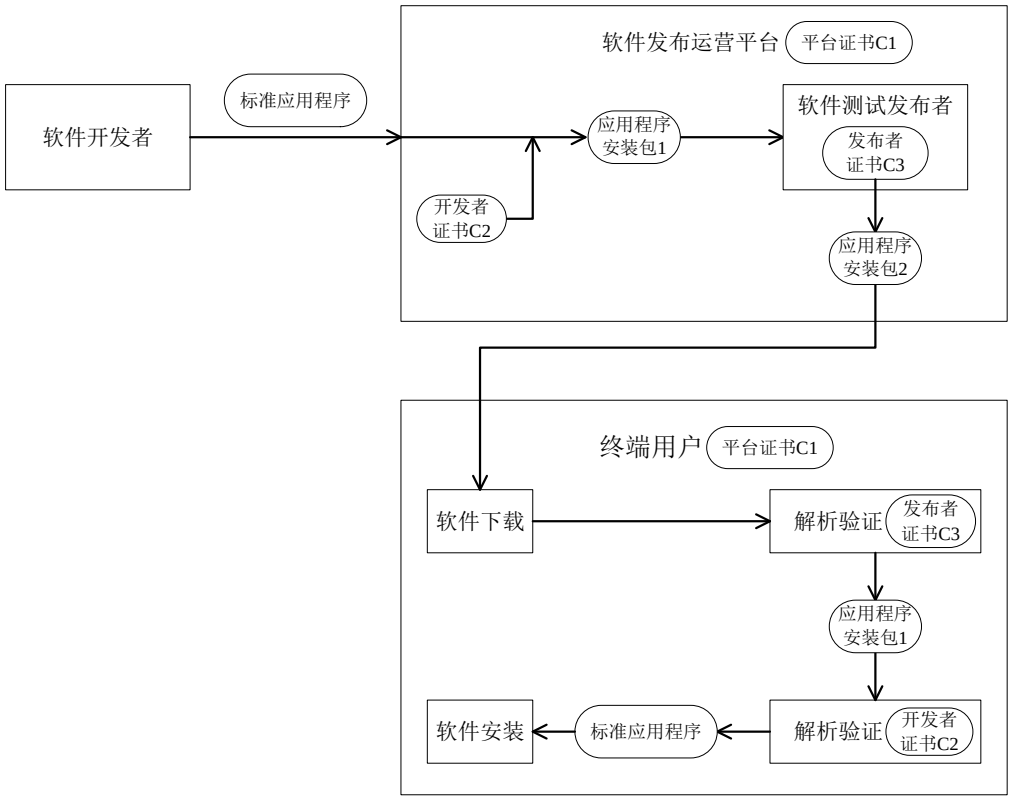



图2：智能电视应用程序安全流程图

整个过程包括两方面的内容：服务端（软件发布运营平台）和设备端（智能电视终端）

**3.4.1 服务端：**

**3.4.1.1 软件发布运营平台生成自身数字证书 C1；**

**3.4.1.2 软件发布运营平台用自身数字证书 C1 为软件开发者、软件发布者签发数字证书 C2 和 C3；**

**3.4.1.3 软件开发者向软件发布运营平台提交标准应用程序；**

**3.4.1.4 软件发布者检测软件开发者提交的应用程序，确认其安全性；**

**3.4.1.5 软件发布运营平台用软件开发者的数字证书 C2 对应用程序签名，并将应用程序和数字证书 C2 打包形成应用程序安装包 1；**

3.4.1.6　软件发布运营平台用软件发布者的数字证书 C3 对应用程序安装包 1 签名 ,将应用程序安装包 1 和软件发布者的数字证书 C3 打包形成应用程序安装包 2；

3.4.1.7　软件发布运营平台发布应用程序安装包 2，提供给终端下载。

3.4.2　设备端：

3.4.2.1　终端预置软件发布平台的数字证书 C1；

3.4.2.2　用户从软件发布运营平台下载或通过其他方式拷贝应用程序安装包 2 到终端；

3.4.2.3　终端解析应用程序安装包 2，获得应用程序安装包 1 和证书 C3，用证书 C1 验证证书 C3；

3.4.2.4　终端解析应用程序安装包 1，获得标准应用程序和证书 C2，用证书 C1 验证证书 C2；

3.4.2.5　如果上述两步验证均通过，终端才能安装标准的应用程序。

## 3.5　支付安全

用户在智能电视终端上进行支付业务时，需要直接调用或通过安全支付中间件调用经过第三方机构认证的支付程序，确保用户支付信息的安全性。同时，对支付应用发送过来的支付请求，由支付中间件与管理后台进行支付鉴权认证，只有认证通过，才能继续进行支付流程。

## 3.6　设备认证安全

系统需要具备对设备合法性进行校验的机制。

## 3.7　API 权限

系统可对 API 的访问权限进行分类控制。用户在安装应用程序时可以授权或者不授权此应用程序请求的权限。

## 3.8　越狱和防篡改

越狱是指用户利用智能电视操作系统的漏洞可以执行管理者权限的任务，包括更新系统，安装非官方应用程序商店的应用，访问系统分区，修改受保护的系统文件，并改变相应的权限等。

为防止发生这种越狱情况，应尽量解决智能电视操作系统存在的隐患，避免应用程序或恶意软件获得超级用户的特权。用户获取 root 权限的系统服务也应该关闭。

防篡改是指用户用来保护关键内容的一种机制，保护对象可以是核心系统库，服务和那些系统运行时不能被修改或损坏的关键数据。

### 3.9 用户数据安全

为防止用户数据误操作到系统安全，用户在智能电视系统中下载或者拷贝的数据，只能放置到指定的区域，其他区域用户无法获取权限。

### 3.10 数据传输安全

所有数据传输需要具有安全性保障。

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。