

中华人民共和国国家标准

GB XXXX—XXXX

互联网电视接收设备技术规范

Technical specification for internet TV receiving device

(报批稿)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

# 目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义、缩略语.....	1
3.1 术语和定义.....	1
3.2 缩略语.....	2
4 技术要求.....	2
4.1 设备用图形符号.....	2
4.2 外观和结构要求.....	2
4.3 功能要求.....	2
4.4 接口要求.....	2
4.5 ITVID 要求.....	3
4.6 总体安全要求.....	3
4.7 硬件平台安全能力要求.....	3
4.8 操作系统安全要求.....	3
4.9 信息内容安全要求.....	4
4.10 应用程序安全要求.....	4
4.11 内容管理安全要求.....	4
4.12 支付安全要求.....	4
5 测试方法.....	4
5.1 测试条件.....	4
5.2 外观和结构检查.....	4
5.3 功能测试.....	4
5.4 接口测试.....	6
5.5 ITVID 测试.....	6
5.6 总体安全要求测试.....	6
5.7 硬件平台安全测试.....	6
5.8 操作系统安全测试.....	7
5.9 信息内容安全测试.....	8
5.10 应用程序安全测试.....	9
5.11 内容管理安全要求.....	9
5.12 支付安全测试.....	9
附录 A（规范性附录） ITVID 格式.....	10

## 前 言

本标准的4.5、4.6、4.9为强制性的，其余为推荐性的。

本标准按照GB/T 1.1-2009和GB/T 20001.10-2014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。

本标准由中华人民共和国工业和信息化部提出并归口。

本标准起草单位：国家广播电视产品质量监督检验中心、中国电子技术标准化研究院、国家广播电视总局广播科学研究院、康佳集团股份有限公司、深圳创维-RGB电子有限公司、青岛海尔多媒体有限公司、四川长虹电器股份有限公司、青岛海信电器股份有限公司、深圳TCL新技术有限公司、中国电子视像行业协会、北京小米电子产品有限公司、天津三星电子有限公司、索尼（中国）有限公司、LG电子（中国）研究开发中心、四川九州电子科技股份有限公司、深圳市海思半导体有限公司、阿里巴巴（中国）有限公司、华为技术有限公司、广州视源电子科技股份有限公司、中国移动通信有限公司研究院、上海索广映像有限公司、红蝶科技（深圳）有限公司、南京熊猫电子股份有限公司、中国电子科技网络信息安全有限公司、工业和信息化部电子第五研究所、清华大学信息技术研究院。

本标准主要起草人：吴昕、潘榕、刘华益、盛志凡、孙齐锋、谢于迪、徐楠、程怡、曹新风、张伟、何广举、李晓榕、崔志龙、周建波、吴超、张文波、张利利、王坤、付云鹏、刘毅、金文成、蒋艳山、杨明磊、邸贺亮、于小博、尹吉成、郭毅峰、陆凯平、王晓虎、阙秀震、朱辉、朱县亮、潘长勇、何聪蕾。

# 互联网电视接收设备技术规范

## 1 范围

本标准规定了互联网电视接收设备的技术要求，描述了相应的测试方法。

本标准适用于支持通过互联网接收广播电视等视听节目的电视接收设备（以下简称“设备”）的开发、测试和生产。其他具备互联网电视接收功能的音视频设备，可参照执行。

## 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。

GB/T 5465.2 电气设备用图形符号 第2部分：图形符号

## 3 术语和定义、缩略语

### 3.1 术语和定义

下列术语和定义适用于本文件。

#### 3.1.1 预置 built-in

在设备出厂前（出厂模式下）预先存储信息内容、安装服务组件或应用程序等内容过程。

#### 3.1.2 出厂设置 factory setting

设备出厂时的默认状态。

#### 3.1.3 互联网电视接收设备 internet TV receiving device

以电视机、显示器、投影机等大型显示屏幕（显示屏幕对角线大于或等于48cm）为显示设备，内置互联网视听节目播放功能的音视频终端设备。

注：包括但不限于机顶盒、电视机、投影机、显示器等产品形态。

#### 3.1.4 端口镜像 port mirroring

在交换机或路由器上，为实现对网络的监听而将一个或多个源端口的数据流转发到某一个指定端口。

注：指定端口也称镜像端口。

#### 3.1.5 校验密钥 proof key

用于进行安全信任链校验的密钥。

#### 3.1.6 信任链 trust chain

自底向上包括硬件系统、引导程序、操作系统和应用程序等环节在内的链路。

### 3.1.7 安全信任链校验机制 security trust chain checking mechanism

信任链中各环节软件能够使用预置在信任链前一环节软件中的对应密钥(其中引导程序使用预置在硬件系统安全存储区内中的校验密钥)进行来源可靠性和完整性校验的安全校验机制。

### 3.2 缩略语

下列缩略语适用于本文件。

DHCP: 动态主机配置协议 (Dynamic Host Configuration Protocol)

HTTP: 超文本传输协议 (Hypertext Transfer Protocol)

ITVID: 互联网电视接收设备标识 (Internet TV Receiving Device Identification)

MAC: 媒体访问控制 (Media Access Control)

NTP: 网络时间协议 (Network Time Protocol)

TCP/IP: 传输控制协议/网络协议 (Transfer Control Protocol/Internet Protocol)

## 4 技术要求

### 4.1 设备用图形符号

图形符号符合GB/T 5465.2的有关规定。

在GB/T 5465.2中未定义的图形符号, 由产品标准规定。

说明功能的文字和图形符号的标志应正确、清晰、端正、牢固, 指示正确。

### 4.2 外观和结构要求

外观整洁, 表面没有凹凸痕、划伤、裂缝、毛刺、霉斑等缺陷, 表面涂镀层无起泡、龟裂、脱落等。金属零件没有锈蚀及其他机械损伤, 灌注物没有外溢。

开关、按键、旋钮的操作应灵活可靠, 零部件紧固无松动。

### 4.3 功能要求

#### 4.3.1 基本功能

支持在互联网上的音视频点播功能, 可支持文字、图片等信息内容。

#### 4.3.2 音视频解码功能

支持的解码音视频格式由产品标准规定。

#### 4.3.3 本地配置

可对网络配置、显示配置、应用程序进行设置。

#### 4.3.4 通信协议

支持的通信协议由产品标准规定。

### 4.4 接口要求

支持的接口由产品标准规定。

## 4.5 ITVID 要求

每台互联网电视接收设备必须具备唯一的ITVID，ITVID必须固化在设备中，不应随用户操作、操作系统版本更新等情况而变更。ITVID必须可在系统信息中查询，设备生产企业必须将ITVID相关信息在产品出厂前报文到行业主管部门指定的平台。

ITVID格式见附录A。

## 4.6 总体安全要求

必须支持安全信任链校验机制。安全信任链各环节（包括引导程序、操作系统、应用程序等）的软件安装和升级操作必须通过基于安全信任链校验机制的安全校验。

## 4.7 硬件平台安全能力要求

### 4.7.1 硬件基础安全能力要求

硬件平台应具备出厂后不可改写的用于存储校验密钥、ITVID等信息的安全存储区域。

### 4.7.2 外部存储设备要求

在插入外部存储设备时，应提示用户。

### 4.7.3 外部无线连接要求

通过无线接口与设备首次连接时，应提示用户，并提供用户控制无线接口的方法。

### 4.7.4 硬件接口安全

硬件调试端口不应向用户开放。

## 4.8 操作系统安全要求

### 4.8.1 启动安全要求

启动时，应基于安全信任链校验机制对引导程序、操作系统逐级进行安全校验，通过安全校验后，方能进入正常工作状态。

### 4.8.2 在线升级

操作系统若有最新版本，应先提示用户是否升级，升级包经安全校验后方可升级，并给出最新版本号和版本更新内容。若需强制升级，应提示并告知用户原因，升级包经安全校验后方可升级。

### 4.8.3 本地升级

应具备系统本地升级功能，升级包经安全校验后方可升级。

### 4.8.4 恢复出厂设置

应具备恢复出厂设置功能，并在恢复出厂设置操作时，给予风险提示。

### 4.8.5 网络安全

出厂时应具备防范计算机病毒、网络入侵和攻击破坏等危害网络安全事项或者行为的基本网络安全功能。

## 4.9 信息内容安全要求

互联网电视接收设备必须符合以下要求：

- a) 必须接入国务院广播电视行政主管部门批准的互联网电视集成平台，禁止接入未经国务院广播电视行政主管部门批准的互联网电视集成平台；
- b) 禁止接入（含链接）各种非法节目源；
- c) 禁止预置法律法规禁止的信息内容（包括但不限于预置图片、文字、菜单、音视频、应用等）；
- d) 禁止后台应用程序开启弹窗等信息推送功能。

## 4.10 应用程序安全要求

应预置和安装符合安全信任链校验机制要求的应用程序。

## 4.11 内容管理安全要求

应具备数字版权管理（DRM）功能。

## 4.12 支付安全要求

若提供付费服务需用户进行支付时，应符合下列规定：

- a) 采用由国家指定的金融机构和合法第三方支付机构提供的安全支付接口，且满足支付机构要求的支付安全保护机制；
- b) 在用户进行支付操作时，能提示所接入支付机构的名称，在用户支付操作完成时，提示用户支付完成。

# 5 测试方法

## 5.1 测试条件

### 5.1.1 测试用标准大气条件

温度：15℃~35℃。

相对湿度：25%~75%。

气压：86 kPa~106 kPa。

### 5.1.2 测试用电源条件

电源：220×（1±10%） V，50×（1±2%） Hz。

### 5.1.3 设备状态设置

设备处于出厂设置状态。若不处于出厂设置状态，恢复出厂设置状态。

## 5.2 外观和结构检查

用目测法和有关检测工具进行外观和结构检查，是否符合4.2的要求。

## 5.3 功能测试

### 5.3.1 视频点播功能测试

#### 5.3.1.1 测试条件

具备10 Mbps及以上的专用网络带宽。

本测试中所使用交换机、无线路由器均处于正常工作状态，测试的视频链接有效，满足设备声明的进行视频点播所需的最低条件。交换机需具备端口镜像功能。

本测试中所使用以太网网络分析设备可为专用的以太网分析仪或以太网络封包分析工具。

### 5.3.1.2 测试步骤

视频点播功能测试系统如图1所示。

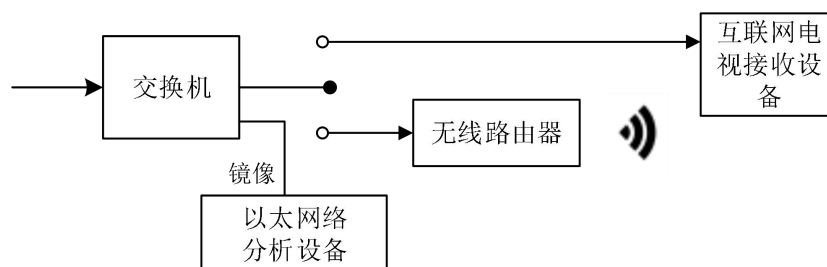


图1 视频点播功能测试系统

视频点播功能测试步骤如下：

- a) 将交换机接入互联网；
- b) 在交换机镜像端口接入以太网网络分析设备；
- c) 若设备具备有线网络接口，则将设备与交换机连接；
- d) 参考说明书，使用设备中的视频点播应用，随机选择其中一个视频进行点播操作；
- e) 若视频正常播放（无马赛克、卡顿等异常情况），则判断为“符合要求”；
- f) 若视频不正常播放（有马赛克、卡顿等异常情况），则判断为“符合要求”，需记录异常情况，并记录以太网网络分析设备中给出的当前网络情况；
- g) 若视频无法播放，记录以太网网络分析设备中给出的当前网络情况，并再随机选择其他不多于4个视频进行点播操作；
- h) 若其中有视频能正常播放（无马赛克、卡顿等异常情况），则按步骤e)进行；
- i) 若其中有视频不正常播放（有马赛克、卡顿等异常情况），则按步骤f)进行；
- j) 若4个视频都无法播放，则判断为“不符合要求”，并记录以太网网络分析设备中给出的当前网络情况；
- k) 若设备具备无线网络接口，则将无线路由器与交换机连接，重复步骤e)～j)；
- l) 若设备不具备有线和无线网络接口，则判断为“不符合要求”。

### 5.3.2 视频解码功能测试

视频解码功能测试步骤如下：

- a) 若设备可接入外部存储设备：
  - 1) 将视频内容存储在设备所支持的外部存储设备中；
  - 2) 将外部存储设备接入设备；
  - 3) 使用企业预置的视频播放器，对声明支持的视频格式进行解码播放；
  - 4) 查看是否能正常播放，若能正常播放则判断为“符合要求”，否则为“不符合要求”。
- b) 若设备不可接入外部存储设备：
  - 1) 由企业指定视频内容读取方式，对声明支持的视频格式进行解码播放；
  - 2) 查看是否能正常播放，若能正常播放则判断为“符合要求”，否则为“不符合要求”。

### 5.3.3 音频解码功能测试

音频解码功能测试步骤如下：

- a) 若设备可接入外部存储设备：
  - 1) 将音频内容存储在设备所支持的外部存储设备中；
  - 2) 将外部存储设备接入设备；
  - 3) 使用企业预置的视频播放器，对声明支持的音频格式进行解码播放；
  - 4) 查看是否能正常播放，若能正常播放则判断为“符合要求”，否则为“不符合要求”。
- b) 若设备不可接入外部存储设备：
  - 1) 由企业指定音频内容读取方式，对声明支持的音频格式进行解码播放；
  - 2) 查看是否能正常播放，若能正常播放则判断为“符合要求”，否则为“不符合要求”。

### 5.3.4 本地配置测试

查看是否可以对网络配置、显示配置、应用程序（如权限管理、更新、卸载等）进行设置。

### 5.3.5 通信协议测试

通过以太网封包分析工具分析设备是否能够支持企业声明支持的通信协议，如TCP/IP、HTTP、DHCP或NTP等。

## 5.4 接口测试

依据产品标准，查看设备是否具备声明支持的接口。若声明接口均支持则判断为“符合要求”，否则为“不符合要求”。

## 5.5 ITVID 测试

ITVID测试步骤如下：

- a) 对设备进行恢复出厂设置，在系统信息中读出设备的 ITVID，查看是否符合附录 A 规定的格式，如果符合附录 A 规定，则进行下一步测试，否则为“不符合要求”；
- b) 查看操作系统是否有升级版本，如果没有，则判定为“符合要求”，如果操作系统有升级版本，对设备进行操作系统升级，在系统信息中读出设备的 ITVID，若两次读出的 ITVID 相同，则判断为“符合要求”，否则为“不符合要求”。

## 5.6 总体安全要求测试

由企业提供安全信任链校验机制的说明，判断信任链中的引导程序、操作系统、应用程序等各环节的软件安装、升级操作是否通过了基于安全信任链校验机制的安全校验。

## 5.7 硬件平台安全测试

### 5.7.1 硬件基础安全能力测试

硬件基础安全能力测试步骤如下：

- a) 由企业提供设备硬件系统具备安全能力的说明；
- b) 若设备硬件系统具备不可改写的存储区域用于存储校验密钥、ITVID 等，则判断为“符合要求”，否则为“不符合要求”。

### 5.7.2 外部存储设备安全测试

外部存储设备安全测试步骤如下：

- a) 等待开机后进入稳定的界面；
- b) 分别插入设备所支持的外部存储设备；
- c) 查看是否每个外部存储设备插入后，都提示用户有外部存储设备接入，若是则判断为“符合要求”，否则为“不符合要求”。

### 5.7.3 外部无线连接安全测试

外部无线连接测试步骤如下：

- a) 等待开机后进入稳定的界面；
- b) 打开设备所支持的一种无线连接方式；
- c) 利用外部无线设备，通过步骤 b) 打开的无线连接方式首次连接设备，查看设备是否提示用户连接到外部无线设备并提供用户控制无线接口的方法；
- d) 若设备支持多种无线连接方式，则重复步骤 b) 和 c)；
- e) 若在每种无线连接方式下，设备都提示用户连接到外部无线设备并提供用户控制无线接口的方法，则判断为“符合要求”，否则为“不符合要求”。

### 5.7.4 硬件接口安全测试

硬件接口安全测试步骤如下：

- a) 由企业提供硬件调试端口安全的说明；
- b) 对企业提供的调试端口进行连接测试，若不能对设备进行调试，则判断为“符合要求”，否则为“不符合要求”。

## 5.8 操作系统安全测试

### 5.8.1 设备启动安全测试

由企业提供安全信任链校验机制的说明，判断引导程序、操作系统启动时是否通过了基于安全信任链校验机制的逐级安全校验，若是则“符合要求”，否则为“不符合要求”。

### 5.8.2 在线升级测试

由企业提供安全信任链校验机制的说明，包括操作系统升级包的校验机制。

- a) **非强制升级**
  - 1) 将设备接入互联网；
  - 2) 查看有无升级提示，有更新时有升级提示信息，且信息中包含升级后版本号信息和是否升级选项；
  - 3) 用户选择升级后，设备下载升级包；
  - 4) 升级包通过校验后，设备能够进行升级并正常启动，核实系统升级后的版本信息；
  - 5) 升级包校验失败后，设备不能升级并正常启动；
  - 6) 上述 1)～5) 测试通过则判断为“符合要求”，否则为“不符合要求”。
- b) **强制升级**
  - 1) 将设备接入互联网；
  - 2) 查看有无升级提示，有更新时有升级提示信息但不具备升级选项，提示信息中包含升级后版本号信息和强制升级原因；
  - 3) 设备下载升级包；

- 4) 升级包通过校验后，设备能够进行升级并正常启动，核实系统升级后的版本信息；
- 5) 升级包校验失败后，设备不能升级并正常启动；
- 6) 上述 1)～5) 测试通过则判断为“符合要求”，否则为“不符合要求”。

c) **手动升级**

- 1) 将设备接入互联网；
- 2) 查看有无升级提示，如无升级提示，用户进行手动检查有无版本更新；
- 3) 有更新时有升级提示信息，且信息中包含升级后版本号信息和是否升级选项；
- 4) 用户选择升级后，设备下载升级包；
- 5) 升级包通过校验后，设备能够进行升级并正常启动，核实系统升级后的版本信息；
- 6) 升级包校验失败后，设备不能升级并正常启动；
- 7) 上述 1)～6) 测试通过则判断为“符合要求”，否则为“不符合要求”；
- 8) 若无版本更新，则由企业协助提供升级。

### 5.8.3 本地升级测试

本地升级功能测试步骤如下：

- a) 若不具备本地升级功能，则判断为“不符合要求”，否则进入下一步测试；
- b) 由企业提供与当前系统不同的完整升级包；
- c) 将需要安装的升级包导入设备，设备安装系统升级包；
- d) 升级包通过校验后，设备能够进行升级并正常启动，核实系统升级后的版本信息；
- e) 升级包校验失败后，设备不能升级并正常启动；
- f) 上述 b)～e) 测试通过则判断为“符合要求”，否则为“不符合要求”。

### 5.8.4 恢复出厂设置测试

出厂设置测试步骤如下：

- a) 查看有无出厂设置，若无则判断为“不符合要求”，否则进入下一步测试；
- b) 进行出厂设置操作，查看有无风险提示，若有则判断为“符合要求”，否则为“不符合要求”。

### 5.8.5 网络安全测试

网络安全测试步骤如下：

- a) 由企业提供具备基本网络安全功能的说明；
- b) 查看是否具备声明的基本网络安全功能，若是，则判断为“符合要求”，否则为“不符合要求”。

## 5.9 信息内容安全测试

信息内容安全测试步骤如下：

- a) 对被测设备进行检查是否连接经国务院广播电视行政主管部门批准的互联网电视集成平台，且没有连接未经国务院广播电视行政主管部门批准的互联网电视集成平台，若是，则判断为“符合要求”，否则判断为“不符合要求”；
- b) 参考说明书，对被测设备连接的节目源进行遍历检查，确认其是否包含非法节目源；
- c) 参考说明书，对被测设备的出厂预置信息内容（包括但不限于预置图片、文字、菜单、音视频、应用等）进行遍历检查，确认其是否包含国家法律法规禁止的信息内容；
- d) 由企业提供设备后台应用程序的控制技术说明，查看设备是否支持后台程序开启弹窗等信息推送功能。

## 5.10 应用程序安全测试

### 5.10.1 预置应用程序安全测试

由企业提供对预置应用程序的安全校验机制说明，确认其是否符合安全信任链校验机制要求，若是则判断为“符合要求”，否则为“不符合要求”。

### 5.10.2 安装应用程序安全测试

安装应用程序安全测试步骤如下：

- a) 由企业指定安装应用程序的方法；
- b) 安装未通过安全校验的应用程序，若无法安装，则判断为“符合要求”，否则为“不符合要求”。

## 5.11 内容管理安全要求

检查设备是否具备数字版权管理功能，若是，则判断为“符合要求”，否则判断为“不符合要求”。

## 5.12 支付安全测试

若预置应用或功能提供付费服务需用户进行支付时，按如下步骤测试：

- a) 操作提供付费服务预置应用或功能；
- b) 查看是否提示所接入支付机构的名称，若是，则进行下一步测试，否则判断为“不符合要求”；
- c) 判断该支付机构是否为中国人民银行许可的金融机构和合法第三方支付机构，若是，则进行下一步测试，否则判断为“不符合要求”；
- d) 判断是否满足支付机构要求的支付安全保护机制，若是，则进行下一步测试，否则判断为“不符合要求”；
- e) 在用户支付操作完成时，检查是否提示用户支付完成，若是，则判断为“符合要求”，否则为“不符合要求”。

附 录 A  
(规范性附录)  
ITVID 格式

ITVID由企业标识+MAC地址+设备类型标识组成，共19个字符。

企业标识共4个字符，为大写字母；MAC地址共12个字符，由16进制数字表示；设备类型标识共3个字符，为大写字母。企业标识由企业提供经ITVID管理机构认可；MAC地址可使用有线网络MAC地址或无线网络MAC地址，首选使用有线网络MAC地址；类型标识DSJ表示设备为电视机类型，JDH为机顶盒，TYJ为投影机，XSQ为显示器，XXX为其他类型。ITVID格式如图A. 1所示。

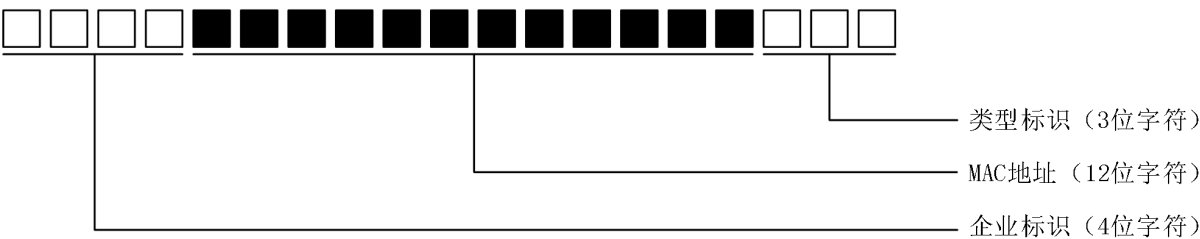


图 A. 1 ITVID 格式