

中华人民共和国国家标准

GB/T XXXXX—XXXX

|  |
| --- |
|  |

信息安全技术 智能家居安全通用技术要求和测试评价方法

Information security technology--General technical requirements of smart home security and testing and evaluation methods

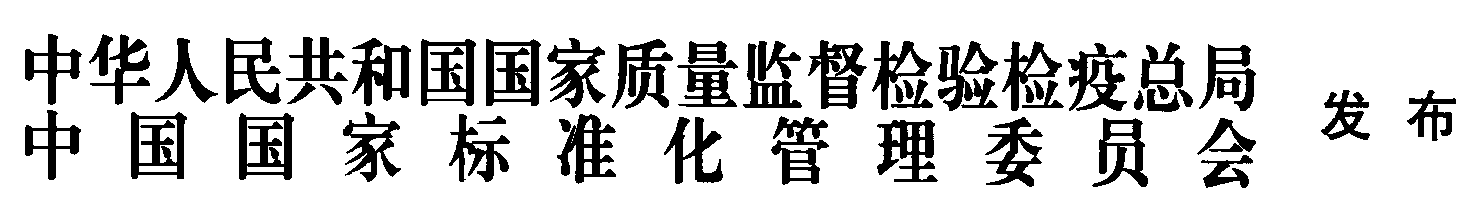
（征求意见稿）

（本稿完成日期：2019/12/08）

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

201X - XX - XX发布

201X - XX - XX实施



ICS XX.XXX

X.XXX

目  次

[前  言 III](#_Toc29311477)

[1范围 1](#_Toc29311478)

[2规范性引用文件 1](#_Toc29311479)

[3术语和定义 1](#_Toc29311480)

[4缩略语 2](#_Toc29311490)

[5智能家居整体框架 3](#_Toc29311534)

[6智能家居安全模型 3](#_Toc29311535)

[7智能家居终端安全要求 4](#_Toc29311536)

[7.1 硬件安全 4](#_Toc29311537)

[7.2 操作系统安全 5](#_Toc29311538)

[7.3 固件升级安全 6](#_Toc29311539)

[7.4 应用安全 6](#_Toc29311540)

[7.5 通信安全 7](#_Toc29311541)

[7.6 数据安全 7](#_Toc29311542)

[7.7个人信息安全 7](#_Toc29311543)

[8智能家居网关安全要求 7](#_Toc29311544)

[8.1 硬件安全 7](#_Toc29311545)

[8.2操作系统安全 7](#_Toc29311546)

[8.3 固件升级安全 7](#_Toc29311547)

[8.4 应用安全 7](#_Toc29311548)

[8.5 通信系统安全 8](#_Toc29311549)

[8.6 数据安全 8](#_Toc29311559)

[8.7 个人信息安全 8](#_Toc29311560)

[9智能家居控制端安全要求 8](#_Toc29311561)

[9.1 硬件安全 8](#_Toc29311562)

[9.2 操作系统安全 8](#_Toc29311563)

[9.3 固件升级安全 9](#_Toc29311564)

[9.4 应用安全 9](#_Toc29311565)

[9.5 通信安全 9](#_Toc29311566)

[9.6 数据安全 9](#_Toc29311567)

[9.7 个人信息安全 9](#_Toc29311568)

[10通信网络安全要求 9](#_Toc29311569)

[10.1网络接入安全 9](#_Toc29311570)

[10.2信令/协议安全 9](#_Toc29311571)

[10.3 网络态势感知安全 9](#_Toc29311572)

[11应用服务平台安全要求 10](#_Toc29311573)

[11.1平台安全 10](#_Toc29311574)

[11.2 应用安全 10](#_Toc29311575)

[11.3 能力调用安全 11](#_Toc29311582)

[11.4 数据安全 11](#_Toc29311583)

[11.5 个人信息安全 12](#_Toc29311584)

[11.6 终端管理安全 12](#_Toc29311585)

[12智能家居安全通用测试评价方法 12](#_Toc29311586)

[12.1 总体说明 12](#_Toc29311587)

[12.2 智能家居终端安全测试评价方法 12](#_Toc29311587)

[12.3 智能家居网关安全测试评价方法 19](#_Toc29311588)

[12.4 智能家居控制端安全测试评价方法 22](#_Toc29311589)

[12.5 通信网络安全测试评价方法 22](#_Toc29311590)

[12.6 应用服务平台安全测试评价方法 24](#_Toc29311592)

[附 录 A （资料性附录） 29](#_Toc29311593)

[A.1 智能家居典型应用场景 29](#_Toc29311594)

[A.2 智能家居安全风险 29](#_Toc29311595)

[A.3 智能家居参与方 29](#_Toc29311596)

[参 考 文 献 31](#_Toc29311597)

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。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：中移（杭州）信息技术有限公司、中国移动通信集团有限公司、中国信息通信研究院、公安部第三研究所、国家计算机网络应急技术处理协调中心、北京京东尚科信息技术有限公司、联想（北京）有限公司、北京百度网讯科技有限公司、阿里巴巴集团控股有限公司、中国电子标准化技术研究院、中国软件评测中心、海信集团有限公司、北京奇虎科技有限公司、深圳市优点科技有限公司、广东欧珀移动通信有限公司、华为技术有限公司、中国网络安全审查技术与认证中心、小米科技有限责任公司、中国信息通信科技集团有限公司、杭州安恒信息技术股份有限公司。

本标准主要起草人：路晓明、张滨、智绪龙、许蓓蓓、邱勤、董靖宇、李轶、贾倩、王华景、乔喆、冯运波、李汝鑫、何清林、张艳、宁华、周毅、刘陶、王剑、王艳红、刘继顺、李笑如、包沉浮、孙科、方强、李世斌、孙宗臣、张屹、汪国平、李腾、姚一楠、衣强、王晖、申永波、李明菊、吴国燕、王辉。

信息安全技术  
智能家居安全通用技术要求和测试评价方法

## 范围

本标准规定了智能家居安全通用技术要求和对应测试评价方法。

本标准适用于智能家居产品的安全设计和实现，智能家居的安全测试和管理也可参照使用。

## 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 25068.3 信息技术 安全技术 IT网络安全 第3部分：使用安全网关的网间通信安全保护

GB/T 25068.4 信息技术 安全技术 IT网络安全 第4部分：远程接入的安全保护

GB/T 25069-2010 信息安全技术 术语

GB/T 29234 基于公用电信网的宽带客户网络安全技术要求

GB/T 31168 信息安全技术 云计算服务安全能力要求

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 36633 信息安全技术 网络用户身份鉴别技术指南

ISO/IEC 27033-6 信息技术 安全技术 网络安全 第6部分 无线IP网络接入安全保护

## 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

### 智能家居 Smart home

以住宅为载体，综合利用网络通讯、多媒体、物联网、人工智能等信息技术，实现家庭设备远程控制、影音娱乐、家庭能源管理、家庭健康等场景化服务的系统。

### 智能家居终端 Smart home terminal

部署在家居环境中，实现智能家居应用功能并协同提供智能家居服务的各类终端设备。

### 智能家居网关 Smart home gateway

在智能家居中实现外部广域通信网络和内部家庭局域网络连通的设备，为智能家居终端分配通信地址，并实现智能家居终端、智能家居应用服务平台和智能家居控制端的网络连接。

### 智能家居控制端 Smart home controller

与智能家居的用户交互，根据接收的用户指令或预先配置的任务，通过智能家居应用服务平台或智能家居网关向智能家居终端发出指令，实现智能家居应用的设备。

### 智能家居应用服务平台 Application service platform of smart home

应用后端智能家居服务应用承载的功能实体，通过与智能家居终端、智能家居控制端协同，实现智能家居的应用服务。

### 控制端应用 Control Application

与网络服务连接，由用户操作能对智能设备进行远程操作的应用程序。

### 设备绑定 Device Binding

操作员对智能家居设备进行网络配置，使其连接到网络中，并申请将其关联到自己账户的行为。

### 安全模块 Security Module

智能家居设备中的硬件模块，为智能家居设备提供密码运算功能，具有受保护的存储空间。

### 关键安全信息 Critical Security Information

与安全相关的秘密信息，这些信息被泄露或被修改后会危及智能家居安全性。例如后台系统管理员认证信息、操作系统登录认证信息，网络设备认证信息等。

## 缩略语

下列缩略语适用于本文件：

|  |  |
| --- | --- |
| API | 应用编程接口（Application Programming Interface） |
| Bin | 二进制文件（Binary File） |
| DDoS | 分布式拒绝服务攻击（Distributed Denial of Service） |
| FTP | 文件传输协议（File Transfer Protocol） |
| ID | 身份标识（Identification） |
| IP | 网络之间互联的协议（Internet Protocol） |
| MAC | 介质访问控制地址（Media Access Control） |
| SSH | 安全外壳协议（Secure Shell） |
| URL | 统一资源定位符（Uniform Resource Locator） |
| VPN | 虚拟专用网络（Virtual Private Network） |
| TEE | 可信执行环境（Trusted Execution Environment） |

## 智能家居整体框架

智能家居是综合利用网络通讯、多媒体、物联网、人工智能等信息技术，实现家庭设备智能控制、信息互动的系统,创造出高效、舒适、安全、便捷的个性化家居生活。智能家居整体框架如图1所示。



图1 智能家居基本框架

智能家居实体包括智能家居用户、智能家居终端、智能家居控制端、智能家居网关、通信网络和智能家居应用服务平台，其中：

1. 智能家居用户即实际使用智能家居服务的终端用户。
2. 智能家居控制端与智能家居用户进行交互，实现对智能家居终端的控制和管理，进而实现智能家居应用。
3. 智能家居网关为智能家居环境提供网络连接，并提供本地场景化服务和设备管理功能
4. 智能家居终端是实现智能家居应用具体功能的设备，为智能家居用户提供感知、数据采集及控制服务。
5. 通信网络分为家庭局域网和互联网，为智能家居提供数据通信连接能力。
6. 智能家居应用服务平台是后端智能家居服务应用承载的功能实体，通过与智能家居终端、智能家居控制端协同，实现智能家居的应用服务。智能家居应用服务平台包含智能家居管理升级功能，通过平台为智能家居终端提供智能家居终端统一管理和固件升级服务。

## 智能家居安全模型

以智能家庭中的设备安全及数据安全为重点保护对象，本标准对智能家居安全模型进行了抽象，如下图2所示。



图2 智能家居安全模型

本标准凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

## 智能家居终端安全要求

### 7.1 硬件安全

#### 7.1.1 硬件接口安全

对于具备硬件接口的设备要求包括：

1. 对于具有console接口的设备，需配置用户名、口令等方式进行认证授权，禁止直接登录，口令应字符长度不少于八位，由大小写字母、数字、特殊符号中的两种或两种以上类型组成。
2. 对于使用无线外围接口的设备，宜通过指示灯或显示屏等方式，提供数据传输状态的监控功能。不同的传输状态应有所差异。
3. 具备调试功能的接口，应在出厂时设置为默认关闭，宜在接口处添加环氧树脂涂层，防止逆向工程。
4. 宜具备数据的物理保护能力，防止攻击者通过去除芯片表面封装层而获取存储器数据。智能家居终端宜具备在受到暴力移除或拆卸时的防护预警机制。

宜具备硬件随机数发生器、密钥生成和加解密运算引擎，加解密运算宜仅在TEE内部处理。

1. 宜具备安全存储区，只有TEE可访问安全存储区。

#### 7.1.2 芯片安全

对于芯片安全要求包括：

1. 对于支持安全模块的芯片，应具备固件芯片的物理写保护的功能，防止固件被篡改。
2. 宜具备安全域隔离功能，提供可信执行环境。
3. 芯片宜使用拆卸存迹硬质涂层，防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。
4. 对于支持安全模块的芯片，宜具备侧信道攻击防护能力。
5. 宜具备安全启动硬件保护能力。

### 7.2 操作系统安全

#### 7.2.1 操作系统集成安全

智能家居终端在进行操作系统集成时，要求包括：

1. 操作系统进行服务裁剪时，应满足模块最小化原则，仅保留必须的模块。
2. 操作系统接口开放时，应仅开放使用端口，关闭非必须端口。
3. 操作系统宜进行安全加固，具备防止逆向工程的能力。

#### 7.2.2操作系统权限限制

对于具备操作系统的智能家居终端要求包括：

1. 对于支持多个用户账号的系统，用户权限分配应遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作。
2. 系统应具备对远程控制的请求身份验证和接入认证的能力，避免非法用户或应用控制系统。
3. 系统在应用安装时需要获得用户授权，未授权或被用户拒绝的应用，系统应拒绝安装。应用安装时，权限分配采取授权最小化原则，系统应能禁止所有未被允许权限的使用。
4. 系统应对不同的应用进程及数据之间实施适当的访问控制管理措施，不同应用程序的进程及数据不能随意互访。
5. 系统不应预留任何未公开帐号，所有帐号应可被操作系统管理。
6. 禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊URL等。

#### 7.2.3 操作系统安全启动认证

宜提供安全启动机制进行系统的完整性保护，当安全验证通过后，系统方能正常启动。

#### 7.2.4 操作系统更新安全机制

对于具备操作系统的智能家居终端要求包括：

1. 应具备操作系统更新机制，且更新前应得到用户确认。
2. 系统更新时，应对更新文件的来源和完整性进行校验。
3. 系统更新失败时，应保证系统的可用性并给予用户相应的提示。
4. 系统应具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。

#### 7.2.5 操作系统配置安全

对于具备操作系统的智能家居终端要求包括：

1. 对具备调试功能的设备，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限滥用。
2. 设备出厂前宜将调试接口默认设置为关闭状态。

#### 7.2.6 服务配置安全

对于具备操作系统的智能家居终端要求包括：

1. 系统服务授权应遵循最小化原则，除必要服务端口以外，尽量减少对外开放端口数量，应默认关闭Telnet和SSH服务端口。
2. 对于能够安装外部应用的系统，应提供对系统API的访问控制机制，防止应用对系统接口的非授权调用。
3. 对于可配置服务的系统，应具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。
4. 系统登录口令宜具有一定复杂度要求，字符长度不少于八位，由大小写字母、数字和特殊符号中两种或两种以上类型组成。
5. 系统宜提供数据通信连接状态的标志。
6. 对于支持远程连接的设备，系统应使用安全的通信协议保障通道安全，包括具备建立通道时的身份鉴别和传输数据的机密性与完整性保护能力。
7. 对于通过Web进行远程管理的设备，对其进行管理和配置的行为必须经过登录认证，其登录/退出过程需有日志记录。记录内容应至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的IP地址等信息。

#### 7.2.7 日志安全

智能家居终端日志功能要求包括：

1. 宜具备记录用户对设备操作的能力，记录包括但不限于以下内容：用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果，且记录应满足GB/T 35273-2017中对个人信息的安全要求。
2. 设备在异常关机、重启、文件系统损坏时产生的告警信息宜自动记入日志。
3. 对于具备文件系统的系统，应具备按帐号分配日志文件读取的能力，防止日志文件被非法读取。仅允许管理员帐号对日志文件进行删除操作。

### 7.3 固件升级安全

对于具备固件的智能家居终端要求包括：

1. 应具备固件更新机制，且更新前应得到用户确认。
2. 对于远程下载升级固件的场景，固件应对更新文件的来源进行校验。
3. 固件下载传输通道应确保可信，防止中间人劫持或者嗅探。
4. 固件升级应具备固件升级文件完整性校验的能力。
5. 固件升级失败，应保持固件可用性。
6. 应支持防止未授权进行固件回退的能力。

### 7.4 应用安全

智能家居终端上的应用要求包括：

1. 宜具备防逆向反编译能力，在安装软件时，智能终端系统宜对安装包的完整性和来源的真实性进行校验。
2. 具备防范越权操控和身份伪冒的能力。
3. 对设备密码、设备认证信息进行加密处理，不应在日志和配置文件中明文记录敏感信息。
4. 如需与智能家居应用服务平台或其他终端应用进行数据交互，则在传输之前应进行双向认证，并且应通过安全的网络传输协议进行通信，保护通信内容的机密性和完整性。
5. 对设备生成和用户输入的用户敏感信息使用安全加密算法进行加密存储。
6. 具备防止对身份验证数据进行暴力攻击破解的能力。
7. 具备对输入数据格式的恶意代码检验能力。
8. 宜支持设备一机一密配置，密钥与设备唯一ID绑定，防止设备伪造。
9. 对于使用传统Bin应用编译宜在编译过程采用安全编译选项，降低内存攻击漏洞的影响。

### 7.5 通信安全

智能家居终端通信要求包括：

1. 对于使用无线接入网络技术的智能家居终端，通信安全见ISO/IEC 27033-6中安全要求。
2. 对于使用家庭宽带有线网络技术的智能家居终端，通信安全见GB/T 29234中的安全要求。
3. 通信配对时应对密钥进行加密传输，防止密钥泄露。

### 7.6 数据安全

对于具备数据收集、传输、存储和访问控制功能的智能家居终端，要求包括：

1. 数据传输时，应用或系统应具备对数据机密性和完整性保护能力，且用于传输加密的密钥不应硬编码在代码中。
2. 对于能够安装第三方应用的系统，应具备对第三方应用软件访问数据权限的控制能力，能够发现或记录非授权应用访问数据。

### 7.7个人信息安全

智能家居终端上的个人信息安全，见GB/T 35273-2017的安全要求。

## 智能家居网关安全要求

### 8.1 硬件安全

智能家居网关应符合7.1硬件安全的要求。

智能家居网关宜具备可信执行环境，保障运行安全。

### 8.2操作系统安全

智能家居网关应符合7.2操作系统安全的要求。

### 8.3 固件升级安全

智能家居网关应符合7.3固件升级安全的要求。

### 8.4 应用安全

智能家居网关应用安全要求包括：

1. 应符合7.4应用安全的要求。
2. 对于支持本地web管理的网关，应具备防护外部攻击能力，支持启动安全策略，如限制连续的非法登录尝试次数。
3. 应对安装包的完整性和来源的真实性进行校验，不应自动安装第三方应用软件。

### 8.5 通信系统安全



#### 8.5.1 接入安全

对于智能家居网关接入安全，应符合7.5通信安全的要求。

#### 8.5.2 智能家居终端接入控制

智能家居终端连接智能家居网关时，对智能家庭网关要求包括：

1. 具备通过MAC地址、管控进行智能家居终端绑定标记和过滤的能力。
2. 支持对接入的智能家居终端进行网络接入权限控制，包括黑白名单控制、限速控制控制等。
3. 支持通过频段、信道划分等安全域划分方式对接入的智能家居终端进行安全隔离。

#### 8.5.3 通信传输安全

智能家居网关应支持安全传输通道功能。



#### 8.5.4 网络攻击防护

智能家居网关的网络攻击防护，要求包括：

1. 智能家居网关宜能够对下挂的智能家居终端开放端口识别，对其中存在风险服务具备告警和屏蔽能力，如Telnet、SSH等服务。
2. 智能家居网关应具备检测外部对家庭设备Telnet请求等异常行为并进行告警及连接阻断的能力。
3. 智能家居网关宜具备防止用户伪造源的组播的能力。
4. 智能家居网关应支持拒绝服务攻击源流量处置能力。
5. 智能家居网关应支持防火墙功能，能够根据策略对特定连接做阻断、限速能够通过远程的方式进行防火墙配置及防护策略下发。
6. 智能家居网关宜具备对通过其传输的流量进行恶意URL/IP、僵木蠕病毒文件检测、告警和拦截的能力。

### 8.6 数据安全

智能家居网关应符合7.6数据安全的要求。

### 8.7 个人信息安全

智能家居网关应符合7.7个人信息安全的要求。

## 智能家居控制端安全要求

### 9.1 硬件安全

对于使用专用硬件设备的智能家居控制端，其硬件安全应符合7.1硬件安全的要求。

### 9.2 操作系统安全

对于使用专用硬件设备，且搭载操作系统的智能家居控制端，其操作系统安全应符合7.2操作系统安全的要求。

### 9.3 固件升级安全

对于使用专用硬件设备，且具备固件的智能家居控制端，其固件升级安全应符合7.3固件升级安全的要求。

### 9.4 应用安全

智能家居控制端上的控制应用要求包括：

1. 具备防逆向反编译能力，对于Android操作系统控制应用，在安装软件时，应对安装包的完整性和来源的真实性进行校验。
2. 具备防范越权操控和身份伪冒的能力。
3. 对用户认证信息进行加密处理，不应在日志和配置文件中明文记录敏感信息。
4. 与智能家居终端之间应通过安全网络协议传输。
5. 如需与智能家居应用服务平台进行数据交互，则在传输之前进行双向认证，并且应通过安全网络协议传输。
6. 对设备上传和用户输入的用户敏感信息应加密存储。
7. 具备防止对身份验证数据进行暴力攻击破解的能力。
8. 卸载时应能删除安装和使用过程中产生的资源文件、配置文件、用户数据和其他临时文件;
9. 控制端应用应确保使用的第三方库和开源组件不存在已公布90天以上的高危及以上等级未处置漏洞，并应具备根据新曝光漏洞自动或手动安装升级补丁的能力;

### 9.5 通信安全

对于智能家居控制端的通信安全，应符合7.5通信安全的要求。

### 9.6 数据安全

对于智能家居控制端的数据安全，应符合7.6数据安全的要求。

### 9.7 个人信息安全

对于智能家居控制端个人信息安全应符合7.7个人信息安全要求。

## 通信网络安全要求

10.1网络接入安全

通信网络接入应满足GB/T 25068.4 的安全要求。

10.2信令/协议安全

通信网络信令/协议安全应满足GB/T 25068.3 的安全要求。

10.3 网络态势感知安全

#### 10.3.1 安全态势分析

网络态势感知中安全态势分析要求包括：

1. 通信网络宜支持对网络中与智能家居相关的脆弱性态势、僵木蠕态势、异常流量态势进行分析。
2. 通信网络宜支持通过威胁情报、安全沙箱等方式，进行威胁收集及分析，为安全态势监测提供数据支持。

#### 10.3.2 网络威胁处置

网络态势感知中网络威胁处置要求包括：

1. 当发现网络中流量异常、僵木蠕大规模爆发等异常时，通信网络应具备一键封堵、流量清洗等方式进行威胁处置。
2. 通信网络应支持对网络攻击进行溯源的能力。

## 应用服务平台安全要求

11.1平台安全

智能家居应用服务平台安全应满足GB/T 31168中的安全要求。

11.2 应用安全



11.2.1 身份鉴别和合法性安全

智能家居应用服务平台应用要求包括：

1. 对使用应用服务平台应用的用户应进行身份鉴别，并满足GB/T 36633中的安全要求。
2. 应用服务平台的应用接入认证，应满足如下安全要求：
3. 构建应用标识体系，为每个应用分配唯一的身份标识。
4. 应对接入平台的应用的身份合法性进行认证，只有经过认证的合法应用才能接入应用服务平台执行后续的业务调用。
5. 应用认证全程不应明文传递密钥或以弱算法等变换后传递，防止反向推出密钥，保证认证安全。
6. 应为不同的应用分配不同的密钥，并支持密钥的生成、分发、存储、更新等密钥管理功能；
7. 对接口的调用都要经过鉴权，限定可操作的资源范围、操作权限。
8. 接入应用服务的设备，应满足如下接入认证安全要求。
   1. 应构建设备标识体系，为每个智能家居终端分配唯一的身份标识，并与设备信息进行关联，如设备厂商、设备类型、型号等信息。
   2. 应通过预置密钥、密钥个人化协商等方式，为每个设备分配唯一的设备密钥，设备密钥与设备标识一一绑定，并支持密钥的生成、分发、存储、更新等密钥管理功能。
   3. 应对接入平台的设备进行身份认证和合法性认证，只有经过认证的设备才能接入业务平台进行后续应用操作。身份认证的方式包括验证PIN码等有效验证用户身份的信息，合法性认证的方法包括基于证书或软件授权验证码的验证等。
   4. 设备认证过程不应明文传递密钥或以弱算法等变换后传递，防止反向推出密钥，保证认证安全。
   5. 设备认证过程如需使用随机数机制，不应使用srand等伪随机算法（时间做种），应使用系统真随机生成，如 /dev/urandom、/dev/random，确保不可预测。
   6. 对于支持应用帐号绑定的设备，不宜通过设备重置方式进行帐号重新绑定，只有原帐号解绑后才可进行重新绑定。
9. 对访问应用服务平台的平台管理人员进行身份鉴别， 宜采用两种或两种以上多因素身份鉴别技术进行身份鉴别，其中一种鉴别技术至少应使用密码技术来实现。

11.2.2 权限控制

智能家居应用服务平台应用，权限控制要求包括：

1. 应支持用户分级分组，并根据不同用户等级、分组授予不同的业务访问权限，只有获得授权的用户，才能访问指定的数据及内容，执行相应应用操作。
2. 应根据不同的应用等级授予不同的应用访问权限，只有获得授权的应用，才能调用指定的应用能力，执行对应的操作。
3. 应根据不同的设备类型或等级授予不同的应用访问权限，只有获得授权的设备，才能访问指定的数据及信息，执行对应的操作。

11.3 能力调用安全

智能家居服务平台间的接口要求包括：

1. 应具备平台与平台之间的合法性校验能力，防止应用服务平台冒用和越权访问。
2. 被调用应用服务平台应具备针对源IP地址范围进行授权的功能，调用该平台时除提供静态口令外还需要对IP地址范围进行授权。
3. 被调用平台应具备对调用平台所调用的资源记录完整操作日志的功能。
4. 对于用户访问权限有要求的接口，应具备访问黑/白名单机制，以便对非法用户访问进行拦截。
5. 应具备恶意攻击的识别与阻断能力。

11.4 数据安全

11.4.1 数据传输安全

对于智能家居应用服务平台之间的数据传输要求包括：

1. 应具备业务平台与智能家居终端、其他业务平台之间的数据机密性保护能力。
2. 应具备业务平台与智能家居终端、其他业务平台之间的数据完整性保护能力，如使用哈希算法、时间戳、计数器等，防止未授权的第三方对数据进行修改、破坏和消息重放等；在存储或传输时应具备数据包排序及差错校验功能，避免信息包的丢失、乱序等。

11.4.2 数据访问控制

对智能家居应用服务平台的数据访问控制要求包括：

1. 应支持权限控制功能，如在虚拟化系统上对于数据库设置不同的访问策略，保证用户仅能对该业务系统对应的数据库进行权限以内的相关操作，不能访问其他未被授权的业务系统数据。
2. 涉及业务机密数据或关键安全信息的文件必须要有权限控制，只能被相应权限的用户访问。
3. 上传下载时，限制用户向上跨目录访问，只能访问指定目录下的文件。

11.4.3 数据存储安全

对智能家居应用服务平台的数据存储要求包括：

1. 应支持分等级的数据加密方法，根据数据密级采用不同的安全存储机制。如对于重要程度低的数据，可以明文存储，保证关键安全信息的保密性。
2. 应支持密钥安全存储，如将密钥存储在加密机或特定代理内部，保证密钥不被泄露。
3. 应支持数据完整性保护，对关键安全信息提供完整性检测机制，关键安全信息损坏和丢失时能够及时发现。
4. 应具备完备的数据备份和恢复功能，一旦发生数据丢失或破坏，可以利用备份恢复数据，保证数据在故障发生后不会丢失。
5. 应具备对各类数据和文件进行归档的能力和定期对临时数据及文件自动清理的功能，数据删除后系统内的文件、目录和数据库等资源所在存储空间被释放或重新分配，应能够支持完全清除，不可恢复。

11.5 个人信息安全

智能家居应用服务平台上的个人信息安全，应满足GB/T 35273-2017的安全要求。

11.6 终端管理安全

对智能家居应用服务平台终端管理要求包括：

1. 应支持设备信息安全上报和指令安全下发，保证上报信息和下发指令的完整性和机密性。
2. 应支持固件安全升级，确保固件升级文件的完整性和机密性，并应对固件来源的真实性进行验证。

## 智能家居安全通用测试评价方法

12.1总体说明

测试方法与技术要求一一对应，在技术要求中，为应的要求对应测评方法中的必选测评项，为宜的建议性要求对应测评方法中的可选测评项，每条技术要求对应的测试评价由检测方法和预期结果组成。

12.2 智能家居终端安全测试评价方法

12.2.1 硬件安全

12.2.1.1 硬件接口安全

硬件接口安全的检测方法和结果判定如下：

1. 检测方法：
   1. 对于具有console接口的设备，检查用户是否需要配置用户名、口令等方式得到认证授权，才能进行登录，是否已禁止直接登录；口令是否使用大小写字母、数字、特殊符号等方式两种或两种以上组成的复杂口令。
   2. 使用无线外围接口传输数据，验证是否具有通过指示灯或显示屏等方式监控数据传输的功能，在不同的传输状态，监控显示是否有差异。
   3. 检查具备调试功能的接口，在出厂时是否设置为默认关闭，是否有环氧树脂涂层；连接调试接口，验证是否可以访问接口，进行逆向工程。
   4. 核查芯片内是否设置光敏检测电路、温度检测电路、电压电路检测、温度检测电路以及频率检测电路等模块，对芯片工作环境进行监控，当攻击者通过去除芯片表面封装层而试图获取存储器数据时，检测模块是否会产生警告信息；或者核查是否对芯片内部总线以及存储器等重要敏感电路部分，添加物理保护层；或者核查是否通过随机振动的电源提高了抗功耗分析攻击的能力。通过暴力移除或者拆卸操作，验证智能家居终端是否具有防护预警机制。
   5. 对智能家居终端进行外部信号干扰，验证智能家居终端是否能稳定工作。
   6. 审查厂商提交的文档，查看是否具备硬件真随机数、硬件加密密钥和加解密引擎，硬件加密密钥只在TEE内部处理。
   7. 审查厂商提交的文档，查看是否具备安全存储区，只有TEE可访问安全存储区。
2. 结果判定：
   1. 对于具有console接口的设备，用户需要配置用户名、口令等方式得到认证授权，才能进行登录，已禁止直接登录；口令使用大小写字母、数字、特殊符号等方式两种或两种以上组成的复杂口令。满足为“符合”，其他情况为“不符合”。
   2. 对于使用无线外围接口的设备，通过指示灯或显示屏等方式，提供数据传输状态的监控功能。不同的传输状态有所差异。满足为“符合”，其他情况为“不符合”。
   3. 具备调试功能的接口，在出厂时设置为默认关闭，在接口处添加环氧树脂涂层，防止逆向工程。满足为“符合”，其他情况为“不符合”。
   4. 芯片具备数据的物理保护能力，防止攻击者通过去除芯片表面封装层而获取存储器数据；智能家居终端具备在受到暴力移除或拆卸时的防护预警机制。满足为“符合”，其他情况为“不符合”。
   5. 智能家居终端的电路设计具备在外部信号扰动下稳定工作能力。满足为“符合”，其他情况为“不符合”。
   6. 具备硬件真随机数、硬件加密密钥和加解密引擎，硬件加密密钥只在TEE内部处理。满足为“符合”，其他情况为“不符合”。
   7. 具备安全存储区，只有TEE可访问安全存储区。满足为“符合”，其他情况为“不符合”。

12.2.1.2 芯片安全

芯片安全的检测方法和结果判定如下：

1. 检测方法：
   1. 对于支持安全模块的芯片，尝试篡改芯片内部固件数据，验证固件芯片是否具有物理写保护的功能。
   2. 审查厂商提交的文档，查看芯片是否具有安全域隔离功能，提供可行执行环境；宜具备安全域隔离功能，提供可信执行环境。
   3. 审查厂商提交的文档，查看芯片是否使用拆卸存迹硬质涂层，可以防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。
   4. 审查厂商提交的文档，查看出厂前是否擦除主控芯片表面的型号、厂商等信息，增加破解难度。
   5. 审查厂商提交的文档，查看是否具备安全启动硬件保护能力。
2. 结果判定：
   1. 支持安全模块的芯片，固件芯片具有物理写保护的功能，防止固件被篡改。满足为“符合”，其他情况为“不符合”。
   2. 芯片具有安全域隔离功能，提供可信执行环境。满足为“符合”，其他情况为“不符合”。
   3. 芯片使用拆卸存迹硬质涂层，防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。满足为“符合”，其他情况为“不符合”。
   4. 出厂前擦除主控芯片表面的型号、厂商等信息，增加破解难度；满足为“符合”，其他情况为“不符合”。
   5. 具备安全启动硬件保护能力。满足为“符合”，其他情况为“不符合”。

12.2.2 操作系统安全

12.2.2.1 操作系统集成安全

操作系统集成安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看操作系统进行服务剪裁时，是否满足模块最小化原则，且仅保留必要的模块。
   2. 检查操作系统接口开发时，是否仅开放使用端口，关闭非必须端口。
   3. 核查操作系统是否进行安全加固，是否具有防止逆向工程的能力。
2. 结果判定：
   1. 操作系统进行服务剪裁时，满足模块最小化原则，仅保留必须的模块。满足为“符合”，其他情况为“不符合”。
   2. 操作系统接口开放时，仅开放使用端口，关闭不当端口。满足为“符合”，其他情况为“不符合”。
   3. 操作系统进行安全加固，具备防止逆向工程的能力。满足为“符合”，其他情况为“不符合”。

12.2.2.2 操作系统权限限制

操作系统权限限制的检测方法和结果判定如下：

1. 检测方法：
   1. 创建多个用户账户，验证用户权限分配是否遵循最小权限原则，普通用户是否只拥有系统赋予的最小权限，尝试越权操作，该越权操作是否被禁止。
   2. 申请远程控制，验证系统是否具有身份认证和接入认证的能力，是否可以禁止非法用户或应用控制系统。
   3. 在系统上申请安装应用，验证是否需要获得用户授权才能安装；如果用户未授权或者用户拒绝安装该应用，系统是否拒绝安装应用。在应用安装时，验证权限分配时，是否采取授权最小化原则，系统是否禁止所有未被允许权限的使用。
   4. 当不同的应用进程或数据之间进行访问时，验证系统是否具有访问控制机制，不同应用程序的进程及数据是否禁止随意互访。
   5. 审查厂商提交的文档，查看系统是否禁止预留任何的未公开帐号，所有帐号都必须可被系统管。
   6. 审查厂商提交的文档，查看是否禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊URL等。
2. 结果判定：
   1. 对于支持多个用户账户的系统，用户权限分配遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作。满足为“符合”，其他情况为“不符合”。
   2. 申请远程控制，系统对远程控制的请求，进行身份验证和接入认证，可以禁止非法用户或应用控制系统。满足为“符合”，其他情况为“不符合”。
   3. 系统在应用安装时需要获得用户授权，未授权或被用户拒绝的应用，系统拒绝安装。应用安装时，权限分配采取授权最小化原则，系统可以禁止所有未被允许权限的使用。满足为“符合”，其他情况为“不符合”。
   4. 系统对不同的应用进程及数据之间实施适当的访问控制管理，不同应用程序的进程及数据不能随意互访。满足为“符合”，其他情况为“不符合”。
   5. 系统禁止预留任何的未公开帐号，所有帐号都必须可被系统管。满足为“符合”，其他情况为“不符合”。
   6. 禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊URL等。满足为“符合”，其他情况为“不符合”。

12.2.2.3 操作系统安全启动认证

操作系统安全启动认证的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看智能家居终端设备是否具有安全启动机制；在非授权的条件下修改启动分区，重新启动操作系统；检查修改的代码是否可以通过完整性验证。
2. 结果判定：
   1. 智能家居终端设备具有安全启动机制，在非授权的条件下修改启动分区，重新启动操作系统，修改后的代码不能通过完整新验证，系统无法正常启动。满足为“符合”，其他情况为“不符合”。

12.2.2.4 操作系统更新安全机制

操作系统更新安全机制的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看操作系统是否具有自动或者手动更新功能；如果具有自动更新功能，在授权的条件下，检查是否可以自动更新操作系统；如果具有手动更新功能，在授权的条件下，检查是否可以手动更新操作系统。
   2. 修改更新文件的来源，在授权的条件下，进行系统更新，检查是否可以通过校验，完成更新；修改更新文件的内容，在授权的条件下，进行系统更新，检查是否可以通过完整性校验，完成更新。
   3. 尝试推送不正确的固件给设备，使升级失败，验证设备是否恢复到之前可用的版本，并提示更新失败的信息。
   4. 审查厂商提交的文档，查看操作系统是否具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。
2. 结果判定：
   1. 操作系统具备自动或者手动更新功能，通过自动或者手动，能够实现操作系统升级。满足为“符合”，其他情况为“不符合”。
   2. 修改更新文件的来源，在授权的条件下，进行系统更新，未通过校验，更新失败；修改更新文件的内容，在授权的条件下，进行系统更新，未通过校验，更新失败。满足为“符合”，其他情况为“不符合”。
   3. 推送不正确的固件给设备，使升级失败，设备可以恢复到之前可用的版本，并提示更新失败的信息。满足为“符合”，其他情况为“不符合”。
   4. 操作系统具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。满足为“符合”，其他情况为“不符合”。

12.2.2.5 操作系统配置安全

操作系统配置安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看具备调试功能的设备，是否限制调试进程在操作系统中的访问权限和操作权限；使用调试进程，进行非授权的访问，检查是否可以访问成功；使用调试进程，进行非授权操作，检查是否操作成功。
   2. 检查出厂前设备是否将调试接口设置为默认关闭状态。
2. 结果判定：
   1. 对具备调试功能的设备，限制调试进程在操作系统中的访问权限和操作权限；使用调试进程，进行非授权访问，访问失败；使用调试进程，进行非授权操作，操作失败。满足为“符合”，其他情况为“不符合”。
   2. 设备出厂前将调试接口设置为默认关闭状态。满足为“符合”，其他情况为“不符合”。

12.2.2.6 服务配置安全

服务配置安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看系统服务授权是否遵循最小化原则，除必要服务端口以外，尽量减少对外开放端口数量，是否默认关闭Telnet和SSH服务端口；在授权的条件下，调用Telnet接口，检查是否可以调用；在授权条件下，调用SSH接口，检查是否可以调用。
   2. 审查厂商提交的文档，查看对于能够安装外部应用的系统，是否提供对系统API的访问控制机制，防止应用对系统接口的非授权调用。
   3. 审查厂商提交的文档，查看对于可配置服务的系统，是否具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。尝试修改服务的默认配置，是否包含修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控，但不限于这些功能。
   4. 将少于八位的弱口令设置为系统登录口令，验证是否设置成功；检查登录口令是否由大小写字母、数字和特殊符号中两种或两种以上类型组成。
   5. 系统进行数据通信时，检查是否有标志显示连接状态。
   6. 对于支持远程连接的设备，验证系统是否使用安全的通信协议保障通道安全；在建立通道时，是否进行身份鉴别；在传输数据时，是否对数据进行机密性与完整性的验证。
   7. 通过Web进行远程管理的设备，对其进行管理和配置时，是否经过登录认证；在登录/退出的过程，是否有日志记录，记录内容是否至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的IP地址等信息。
2. 结果判定：
   1. 系统服务授权遵循最小化原则，除必要服务端口以外，尽量减少对外开放端口数量，默认关闭Telnet和SSH服务端口；在授权的条件下，调用Telnet接口，调用失败；在授权条件下，调用SSH接口，调用失败。满足为“符合”，其他情况为“不符合”。
   2. 对于能够安装外部应用的系统，提供对系统API的访问控制机制。满足为“符合”，其他情况为“不符合”。
   3. 对于可配置服务的系统，具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。满足为“符合”，其他情况为“不符合”。
   4. 将少于八位的弱口令设置为系统登录口令，设置不成功；登录口令由大小写字母、数字和特殊符号中两种或两种以上类型组成。满足为“符合”，其他情况为“不符合”。
   5. 系统进行数据通信时，有标志显示连接状态。满足为“符合”，其他情况为“不符合”。
   6. 对支持远程连接的设备，系统使用安全的通信协议保障通道安全；在建立通道时，必须进行身份鉴别；在传输数据时，对数据进行机密性与完整性的验证。满足为“符合”，其他情况为“不符合”。
   7. 通过Web进行远程管理的设备，对其进行管理和配置时，必须经过登录认证；日志记录登录/退出的过程，记录内容至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的IP地址等信息。满足为“符合”，其他情况为“不符合”。

12.2.2.7 日志安全

日志安全的检测方法和结果判定如下：

1. 检测方法：
   1. 当用户对设备进行操作时，检查是否进行了日志记录，记录内容是否至少包含用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果，且记录应符合GB/T 35273-2017中对个人信息的安全要求。
   2. 检查设备在异常关机、重启、文件系统损坏时产生的告警信息，是否自动记入日志。
   3. 对于具备文件系统的系统，检查是否具备按账号分配日志文件读取的能力，尝试使用其他合法账户读取现在账户的日志文件，检查是否可以读取；使用非超级管理员账户对日志文件进行删除操作，检查是否删除成功。
2. 结果判定：
   1. 当用户对设备进行操作时，设备对其进行了日志记录，记录内容至少包含用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果，且记录应符合GB/T 35273-2017中对个人信息的安全要求。满足为“符合”，其他情况为“不符合”。
   2. 设备在异常关机、重启、文件系统损坏时产生的告警信息，自动记入日志。满足为“符合”，其他情况为“不符合”。
   3. 对于具备文件系统的系统，具备按账号分配日志文件读取的能力，使用其他合法账户读取现在账户的日志文件，读取失败；使用非超级管理员账户对日志文件进行删除操作，删除失败。满足为“符合”，其他情况为“不符合”。

12.2.3 固件升级安全

固件安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看操作系统是否具有自动和手动更新功能；如果具有自动更新功能，在授权的条件下，检查是否可以自动更新操作系统；如果具有手动更新功能，在授权的条件下，检查是否可以手动更新操作系统。
   2. 在升级服务器中添加用于测试的新版本固件,启动固件升级,检查固件升级前是否对固件升级包验证来源可靠性。
   3. 审查厂商提交的文档，查看固件下载链路是否可确保可信，防止中间人劫持或者嗅探。
   4. 修改固件升级文件的内容，在授权的条件下，进行系统更新，检查是否可以通过完整性校验，完成更新。
   5. 尝试推送不正确的固件给设备，使升级失败，验证设备是否恢复到之前可用的版本。
2. 结果判定：
   1. 操作系统具有自动和手动更新功能。满足为“符合”，其他情况为“不符合”。
   2. 在升级服务器中添加用于测试的新版本固件,启动固件升级,固件升级前对固件升级包验证来源可靠性。满足为“符合”，其他情况为“不符合”。
   3. 固件下载链路可以确保可信，防止中间人劫持或者嗅探。满足为“符合”，其他情况为“不符合”。
   4. 修改固件升级文件的内容，在授权的条件下，进行系统更新，不能通过完整性校验，更新失败。满足为“符合”，其他情况为“不符合”。
   5. 推送不正确的固件给设备，使升级失败，设备可以恢复到之前可用的版本。满足为“符合”，其他情况为“不符合”。

12.2.4 应用安全

应用安全的测试评价方法如下：

1. 测试方法：
   1. 检查应用是否具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。
   2. 尝试越权操作，检查是否可以操作；尝试非法身份操作，检查是否可以操作。
   3. 检查在日志和配置文件中，是否明文记录设备密码、设备认证信息。
   4. 与智能家居应用服务平台进行数据交互时，检查在传输之前是否进行双向认证，并且在通信时是否采用安全网络协议。
   5. 检查对设备生成和用户输入的用户敏感信息是否使用安全加密算法加密存储。
   6. 检查是否具有防止身份验证数据被暴力攻击的能力。
   7. 检查是否具备对输入数据格式的恶意代码检验能力，输入不安全的数据，是否会进行过滤处理。
   8. 审查厂商提交的文档，查看是否禁止使用业界已知的不安全的密码算法。
2. 结果判定；
   1. 应用具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。满足为“符合”，其他情况为“不符合”。
   2. 对应用进行越权操作，操作失败；使用非法身份操作，操作失败。满足为“符合”，其他情况为“不符合”。
   3. 在日志和配置文件中，对设备密码、设备认证信息进行加密存储。满足为“符合”，其他情况为“不符合”。
   4. 与智能家居应用服务平台进行数据交互时，在传输之前进行双向认证，并且在通信时采用安全网络协议。满足为“符合”，其他情况为“不符合”。
   5. 对设备生成和用户输入的用户敏感信息使用安全加密算法加密存储。满足为“符合”，其他情况为“不符合”。
   6. 具有防止身份验证数据被暴力攻击的能力。满足为“符合”，其他情况为“不符合”。
   7. 具备对输入数据格式的恶意代码检验能力，输入不安全的数据，会进行过滤处理。满足为“符合”，其他情况为“不符合”。
   8. 禁止使用业界已知的不安全的密码算法。满足为“符合”，其他情况为“不符合”。

12.2.5 通信安全

通信安全的测试评价方法与预期结果如下：

1. 测试评价方法：
   1. 对于使用无线接入网络技术的智能家居终端，查看客户是否能提供ISO/IEC 27033-6中对于无线IP网络接入对应项的符合性证明。
   2. 对于使用家庭宽带有线网络技术的智能家居终端，查看客户是否提供GB/T 29234中对于宽带有线网络接入对应项的符合性证明。
2. 预期结果：
   1. 对于使用无线接入网络技术的智能家居终端，客户提供的证明，符合ISO/IEC 27033-6中对于无线IP网络接入的安全要求。满足为“符合”，其他情况为“不符合”。
   2. 对于使用家庭宽带有线网络技术的智能家居终端，客户提供的证明，符合GB/T 29234中对于宽带有线网络接入的安全要求。满足为“符合”，其他情况为“不符合”。

12.2.6 数据安全

数据安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看在数据传输时，应用或系统是否具备对敏感数据进行保护的能力，保障关键安全信息的机密性、完整性和有效性，用于传输加密的密钥不是硬编码在代码中；扫描设备的通信端口,检查是否能获取敏感信息。
   2. 对于数据库连接密码、FTP服务密码、登录密码、外部系统接口认证密码等关键安全信息，检查是否加密并单独存储。
   3. 对于能够安装第三方应用的系统，检查是否具备对第三方应用软件访问数据权限的控制能力，进行非授权访问数据，是否能够发现或记录该操作。
   4. 审查厂商提交的文档，查看是否禁止使用业界已知的不安全的密码算法或通信传输协议和加密算法。
2. 结果判定：
   1. 在数据传输时，应用或系统具备对敏感数据进行保护的能力，保障关键安全信息的机密性、完整性和有效性，用于传输加密的密钥不是硬编码在代码中；扫描设备的通信端口,不能获取敏感信息。满足为“符合”，其他情况为“不符合”。
   2. 对于数据库连接密码、FTP服务密码、登录密码、外部系统接口认证密码等关键安全信息，加密并单独存储。满足为“符合”，其他情况为“不符合”。
   3. 对于能够安装第三方应用的系统，具备对第三方应用软件访问数据权限的控制能力，进行非授权访问数据，能够发现或记录该操作。满足为“符合”，其他情况为“不符合”。
   4. 禁止使用业界已知的不安全的密码算法或通信传输协议。满足为“符合”，其他情况为“不符合”。

12.2.7 个人信息安全

个人信息安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 35273-2017标准中对应项的符合性证明。
2. 结果判定：
   1. 客户提供的证明，符合GB/T 35273-2017标准中要求。满足为“符合”，其他情况为“不符合”。

### 12.3 智能家居网关安全测试评价方法

12.3.1 硬件安全

硬件接口安全的检测方法和结果判定参照12.2.1。

12.3.2 操作系统安全

操作系统安全的检测方法和结果判定参照12.2.2。

12.3.3 固件升级安全

固件升级安全的检测方法和结果判定参照12.2.3。

12.3.4 应用安全

应用安全的测试评价方法如下：

1. 测试方法：
   1. 检查应用是否具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。
   2. 尝试越权操作，检查是否可以操作；尝试非法身份操作，检查是否可以操作。
   3. 检查在日志和配置文件中，是否明文记录设备密码、设备认证信息。
   4. 与智能家居应用服务平台进行数据交互时，检查在传输之前是否进行双向认证，并且在通信时是否采用安全网络协议。
   5. 检查对设备生成和用户输入的用户敏感信息是否使用安全加密算法加密存储。
   6. 检查是否具有防止身份验证数据被暴力攻击的能力。
   7. 检查是否具备对输入数据格式的恶意代码检验能力，输入不安全的数据，是否会进行过滤处理。
   8. 审查厂商提交的文档，查看是否禁止使用业界已知的不安全的密码算法。
   9. 审查厂商提交的文档，查看对于支持本地web管理的网关，是否满足登录错误次数限制等安全要求；尝试错误登录，达到规定错误次数时，验证设备是否采取相应安全措施。
2. 结果判定：
   1. 应用具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。满足为“符合”，其他情况为“不符合”。
   2. 对应用进行越权操作，操作失败；使用非法身份操作，操作失败。满足为“符合”，其他情况为“不符合”。
   3. 在日志和配置文件中，对设备密码、设备认证信息进行加密存储。满足为“符合”，其他情况为“不符合”。
   4. 与智能家居应用服务平台进行数据交互时，在传输之前进行双向认证，并且在通信时采用安全网络协议。满足为“符合”，其他情况为“不符合”。
   5. 对设备生成和用户输入的用户敏感信息使用安全加密算法加密存储。满足为“符合”，其他情况为“不符合”。
   6. 具有防止身份验证数据被暴力攻击的能力。满足为“符合”，其他情况为“不符合”。
   7. 具备对输入数据格式的恶意代码检验能力，输入不安全的数据，会进行过滤处理。满足为“符合”，其他情况为“不符合”。
   8. 禁止使用业界已知的不安全的密码算法。满足为“符合”，其他情况为“不符合”。
   9. 对于支持本地web管理的网关，满足登录错误次数限制等安全要求。满足为“符合”，其他情况为“不符合”。

12.3.5 通信系统安全

12.3.5.1 接入安全

接入安全的测试评价方法与预期结果如下：

1. 测试评价方法：
   1. 对于使用无线接入网络技术的智能家居终端，通信安全应满足ISO/IEC 27033-6中对于无线IP网络接入的安全要求。
   2. 对于使用家庭宽带有线网络技术的智能家居终端，通信安全应满足GB/T 29234中对于宽带有线网络接入的安全要求。
2. 预期结果：
   1. 对于使用无线接入网络技术的智能家居终端，客户提供的证明，符合ISO/IEC 27033-6中对于无线IP网络接入的安全要求。满足为“符合”，其他情况为“不符合”。
   2. 对于使用家庭宽带有线网络技术的智能家居终端，客户提供的证明，符合GB/T 29234中对于宽带有线网络接入的安全要求。满足为“符合”，其他情况为“不符合”。

12.3.5.2 智能家居终端接入控制

终端接入控制的测试评价方法与预期结果如下：

1. 测试评价方法：
   1. 审查厂商提交的文档，查看是否具备通过MAC地址、管控进行智能家居终端绑定标记和过滤的能力。
   2. 审查厂商提交的文档，查看是否支持对接入的智能家居终端进行网络接入权限控制，包括黑白名单控制、限速控制、访问时长控制等；尝试设置黑白名单控制、限速控制、访问时长控制等。
   3. 审查厂商提交的文档，查看是否支持通过安全域划分、频段、信道划分等安全域划分方式对接入的智能家居终端进行安全隔离。
2. 预期结果：
   1. 具备通过MAC地址、管控进行智能家居终端绑定标记和过滤的能力。满足为“符合”，其他情况为“不符合”。
   2. 支持对接入的智能家居终端进行网络接入权限控制，包括黑白名单控制、限速控制、访问时长控制等；可以设置黑白名单控制、限速控制、访问时长控制等。满足为“符合”，其他情况为“不符合”。
   3. 支持通过安全域划分、频段、信道划分等安全域划分方式对接入的智能家居终端进行安全隔离。满足为“符合”，其他情况为“不符合”。

12.3.5.3 通信传输安全

通信传输安全的测试评价方法与预期结果如下：

1. 测试评价方法：
   1. 审查厂商提交的文档，查看智能家居网关是否支持安全通道能力，符合GB/T 25068.3-2010的安全要求。
2. 预期结果：
   1. 智能家居网关支持VPN安全通道能力，见GB/T 25068.3-2010的安全要求。满足为“符合”，其他情况为“不符合”。

12.3.5.4 网络攻击防护

网络攻击防护的测试评价方法与预期结果如下：

1. 测试评价方法：
   1. 尝试在智能家居网关中，下挂非法终端，验证其是否可以识别存在风险的服务，并告警和屏蔽，如Telnet、SSH等服务。
   2. 尝试对家庭设备Telnet请求，验证智能家居网关是否可以检测到这种异常行为并进行告警及连接阻断的能力。
   3. 尝试进行用户伪造源的组播，验证智能家居网关是否可以组织这种行为。
   4. 审查厂商提交的文档，查看智能家居网关是否支持拒绝服务攻击源流量清洗功能，对内部输出的异常流量进行检测和处置能力。
   5. 审查厂商提交的文档，查看智能家居网关是否支持防火墙功能，能够根据策略对特定连接做阻断、限速能够通过远程的方式进行防火墙配置及防护策略下发。
   6. 尝试对通过智能家居网关传输的流量进行恶意URL/IP、僵木蠕病毒文件攻击，验证其是否可以检测、告警和拦截。
2. 预期结果：
   1. 在智能家居网关中，下挂非法终端，其可以识别存在风险的服务，并告警和屏蔽，如Telnet、SSH等服务。满足为“符合”，其他情况为“不符合”。
   2. 对家庭设备Telnet请求，智能家居网关可以检测到这种异常行为并进行告警及连接阻断的能力。满足为“符合”，其他情况为“不符合”。
   3. 进行用户伪造源的组播，智能家居网关可以组织这种行为。满足为“符合”，其他情况为“不符合”。
   4. 智能家居网关支持拒绝服务攻击源流量清洗功能，对内部输出的异常流量进行检测和处置能力。满足为“符合”，其他情况为“不符合”。
   5. 智能家居网关支持防火墙功能，能够根据策略对特定连接做阻断、限速能够通过远程的方式进行防火墙配置及防护策略下发。满足为“符合”，其他情况为“不符合”。
   6. 对通过智能家居网关传输的流量进行恶意URL/IP、僵木蠕病毒文件攻击，其可以检测、告警和拦截。满足为“符合”，其他情况为“不符合”。

12.3.6 数据安全

数据安全的检测方法和结果判定参照12.2.6。

12.3.7 个人信息安全

个人信息安全的检测方法和结果判定参照12.2.7。

### 12.4 智能家居控制端安全测试评价方法

智能家居控制端硬件安全、操作系统安全、固件升级安全、通信系统安全、数据安全、个人信息安全的检测方法和结果判定参照12.2.1、12.2.2、12.2.3、12.2.5、12.2.6、12.2.7要求。

12.4.1应用安全

控制端应用安全的测试评价方法如下：

1. 测试方法：
   1. 检查控制端应用是否具备防伪冒、防应用二次打包/篡改、防逆向反编译功能。
   2. 尝试越权操作，检查是否可以操作；尝试非法身份操作，检查是否可以操作。
   3. 检查在日志和配置文件中，是否明文记录用户密码、用户认证信息。
   4. 检查与智能家居终端之间通信数据是否通过安全网络协议传输。
   5. 与智能家居应用服务平台进行数据交互时，检查在传输之前是否进行双向认证，并且在通信时，是否采用安全网络协议传输。
   6. 检查对设备生成和用户输入的用户敏感信息是否加密存储。
   7. 检查是否具有防止身份验证数据被暴力破解的能力。
   8. 卸载应用，检查是否删除安装和使用过程中产生的资源文件、配置文件、用户数据和其他临时文件。
   9. 检查控制端应用使用的第三方库和开源组件是否不存在已公布90天以上的高的高危漏洞；具备根据新曝光漏洞自动或手动安装升级补丁的能力。
2. 结果判定：
   1. 控制端应用具备防伪冒、防应用二次打包/篡改、防逆向反编译功能。满足为“符合”，其他情况为“不符合”。
   2. 越权操作，不可以被执行；非法身份操作，不可以被执行。满足为“符合”，其他情况为“不符合”。
   3. 在日志和配置文件中，不存在明文记录设备密码、设备认证信息。满足为“符合”，其他情况为“不符合”。
   4. 与智能家居终端之间通过安全网络协议传输。满足为“符合”，其他情况为“不符合”。
   5. 与智能家居应用服务平台进行数据交互时，在传输之前进行双向认证，并且通过安全网络协议传输。满足为“符合”，其他情况为“不符合”。
   6. 对设备生成和用户输入的用户敏感信息加密存储。满足为“符合”，其他情况为“不符合”。
   7. 具有防止身份验证数据被暴力破解的能力。满足为“符合”，其他情况为“不符合”。
   8. 卸载应用时，应用会删除安装和使用过程中产生的资源文件、配置文件、用户数据和其他临时文件。满足为“符合”，其他情况为“不符合”。
   9. 控制端应用确保使用的第三方库和开源组件不存在已公布30天以上的高危及以上等级漏洞，并具备根据新曝光漏洞自动或手动安装升级补丁的能力。满足为“符合”，其他情况为“不符合”。

### 12.5 通信网络安全测试评价方法

12.5.1 网络接入安全

网络接入安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 25068.4 标准中对应项的符合性证明。
2. 结果判定：
   1. 客户提供的证明，符合GB/T 25068.4 标准中要求。满足为“符合”，其他情况为“不符合”。

12.5.2 信令/协议安全

网络接入安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 25068.3标准中对应项的符合性证明。
2. 结果判定：
   1. 客户提供的证明，符合GB/T 25068.3标准中要求。满足为“符合”，其他情况为“不符合”。

12.5.3 网络态势感知安全

#### 12.5.3.1 安全态势分析

安全态势分析的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看通信网络是否支持对网络中与智能家居相关的脆弱性态势、僵木蠕态势、异常流量态势进行分析。
   2. 审查厂商提交的文档，查看通信网络是否支持通过威胁情报、安全沙箱等方式，进行威胁收集及分析，为安全态势监测提供数据支持。
2. 结果判定：
   1. 通信网络支持对网络中与智能家居相关的脆弱性态势、僵木蠕态势、异常流量态势进行分析。满足为“符合”，其他情况为“不符合”。
   2. 通信网络支持通过威胁情报、安全沙箱等方式，进行威胁收集及分析，为安全态势监测提供数据支持。满足为“符合”，其他情况为“不符合”。

#### 12.5.3.2 网络威胁处置

网络威胁处置的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看当发现网络中流量异常、僵木蠕大规模爆发等异常时，通信网络是否具备一键封堵、流量清洗等方式进行威胁处置。
   2. 审查厂商提交的文档，查看通信网络是否支持对网络攻击进行溯源的能力。
2. 结果判定：
   1. 当发现网络中流量异常、僵木蠕大规模爆发等异常时，通信网络具备一键封堵、流量清洗等方式进行威胁处置。满足为“符合”，其他情况为“不符合”。
   2. 通信网络支持对网络攻击进行溯源的能力。满足为“符合”，其他情况为“不符合”。

### 12.6 应用服务平台安全测试评价方法

12.6.1 平台安全

平台安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 31168标准中对应项的符合性证明。
2. 结果判定：
   1. 客户提供的证明，符合GB/T 31168 标准中要求。满足为“符合”，其他情况为“不符合”。

12.6.2 应用安全

12.6.2.1 身份鉴别安全

身份鉴别安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 36633标准中对应项的符合性证明。
   2. 应用服务平台的应用接入认证，检测方法如下：
2. 审查厂商提交的文档，查看是否构建应用标识体系，为每个应用分配唯一的身份标识；
3. 尝试将非法应用，接入到平台，检查平台是否进行应用合法性身份认证，是否只有经过认证的合法应用才能接入应用服务平台执行后续的业务调用。
4. 应用认证中，检查全程是否明文传递密钥或以弱算法等变换后传递。
5. 审查厂商提交的文档，查看是否为不同的应用分配不同的密钥，并支持密钥的生成、分发、存储、更新等密钥管理功能。
6. 审查厂商提交的文档，查看对接口的调用是否都要经过鉴权，限定可操作的资源范围、操作权限。
   1. 接入应用服务的设备，检测方法如下：
7. 审查厂商提交的文档，查看是否构建设备标识体系，为每个智能家居终端分配唯一的身份标识，并与设备信息进行关联，如设备厂商、设备类型、型号等信息。
8. 审查厂商提交的文档，查看是否通过预置密钥、密钥个人化协商等方式，为每个设备分配唯一的设备密钥，设备密钥与设备标识一一绑定，并支持密钥的生成、分发、存储、更新等密钥管理功能。
9. 尝试将设备接入平台，检查平台是否对其进行身份认证，是否只有经过认证的合法设备才能接入业务平台进行后续应用操作。
10. 审查厂商提交的文档，查看设备认证过程是否明文传递密钥或以弱算法等变换后传递。
    1. 审查厂商提交的文档，查看对访问应用服务平台的平台管理人员是否进行身份鉴别，是否采用两种或两种以上组合身份鉴别技术进行身份鉴别，其中一种鉴别技术至少使用密码技术来实现；尝试平台管理员访问应用服务平台，检查是否进行身份鉴别。
11. 结果判定：
    1. 客户提供的证明，符合GB/T 36633 标准中要求。满足为“符合”，其他情况为“不符合”。
    2. 应用服务平台的应用接入认证，结果判定如下：
12. 构建应用标识体系，为每个应用分配唯一的身份标识。
13. 将非法应用，接入到平台，平台进行应用合法性身份认证，只有经过认证的合法应用才能接入应用服务平台执行后续的业务调用。
14. 应用认证中，全程不存在明文传递密钥或以弱算法等变换后传递。
15. 为不同的应用分配不同的密钥，并支持密钥的生成、分发、存储、更新等密钥管理功能。
16. 对接口的调用都要经过鉴权，限定可操作的资源范围、操作权限。
17. 以上均满足为“符合”，其他情况为“不符合”。
    1. 接入应用服务的设备，结果判定如下：
18. 构建设备标识体系，为每个智能家居终端分配唯一的身份标识，并与设备信息进行关联，如设备厂商、设备类型、型号等信息。
19. 通过预置密钥、密钥个人化协商等方式，为每个设备分配唯一的设备密钥，设备密钥与设备标识一一绑定，并支持密钥的生成、分发、存储、更新等密钥管理功能。
20. 将设备接入平台，检查平台对其进行身份认证，只有经过认证的合法设备才能接入业务平台进行后续应用操作。
21. 设备认证过程不存在明文传递密钥或以弱算法等变换后传递。

以上均满足为“符合”，其他情况为“不符合”。

* 1. 对访问应用服务平台的平台管理人员进行身份鉴别，采用两种或两种以上组合身份鉴别技术进行身份鉴别，其中一种鉴别技术至少使用密码技术来实现别。足为“符合”，其他情况为“不符合”。

12.6.2.2 权限控制

权限控制的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看是否支持用户分级分组，并根据不同用户等级、分组授予不同的业务访问权限，是否只有获得授权的用户，才能访问指定的数据及内容，执行相应应用操作；验证是否只有获得授权的用户，才能访问指定的数据及内容，执行相应应用操作；
   2. 审查厂商提交的文档，查看是否根据不同的应用等级授予不同的应用访问权限，只有获得授权的应用，才能调用指定的应用能力，执行对应的操作。验证是否根据不同的应用等级授予不同的应用访问权限，只有获得授权的应用，才能调用指定的应用能力，执行对应的操作。
   3. 审查厂商提交的文档，查看是否根据不同的设备类型或等级授予不同的应用访问权限，只有获得授权的设备，才能访问指定的数据及信息，执行对应的操作。验证是否根据不同的设备类型或等级授予不同的应用访问权限，只有获得授权的应用，才能访问指定的数据及信息，执行对应的操作。
2. 结果判定：
   1. 支持用户分级分组，并根据不同用户等级、分组授予不同的业务访问权限，只有获得授权的用户，才能访问指定的数据及内容，执行相应应用操作。
   2. 根据不同的应用等级授予不同的应用访问权限，只有获得授权的应用，才能调用指定的应用能力，执行对应的操作。
   3. 根据不同的设备类型或等级授予不同的应用访问权限，只有获得授权的设备，才能访问指定的数据及信息，执行对应的操作。
   4. 1）-3）项满足为“符合”，其他情况为“不符合”。

12.6.3 能力调用安全

能力调用安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看是否具备平台与平台之间的合法性校验能力，防止应用服务平台冒用和越权访问；尝试使用非法应用服务平台，查看是否可以访问合法平台。
   2. 查看被调用应用服务平台应是否具备针对源IP地址范围进行授权的功能，验证调用该平台时，验证是否除提供静态口令外还需要对IP地址范围进行授权。
   3. 尝试合法平台调用另一合法平台的资源，查看被调用平台是否具备对调用平台所调用的资源记录完整操作日志的功能。
   4. 审查厂商提交的文档，查看对于用户访问权限有要求的接口，是否具备访问黑/白名单机制，以便对非法用户访问进行拦截。尝试非法用户访问接口，查看是否被拦截。
2. 结果判定：
   1. 具备平台与平台之间的合法性校验能力；使用非法应用服务平台，不可以访问合法平台；
   2. 被调用应用服务平台应具备针对源IP地址范围进行授权的功能。足为“符合”，其他情况为“不符合”。
   3. 合法平台调用另一合法平台的资源，被调用平台具备对调用平台所调用的资源记录完整操作日志的功能。足为“符合”，其他情况为“不符合”。
   4. 对于用户访问权限有要求的接口，具备访问黑/白名单机制，以便对非法用户访问进行拦截。足为“符合”，其他情况为“不符合”。

12.6.4 数据安全

12.6.4.1 数据传输安全

数据传输安全的检测方法和结果判定如下：

1. 检测方法：
   1. 验证对业务平台与智能家居终端、其他业务平台之间的关键安全信息（敏感信息包括后台系统管理员认证信息、操作系统登录认证信息，网络设备认证信息等）是否进行加密保护。
   2. 验证对业务平台与智能家居终端、其他业务平台之间的关键安全信息是否进行完整校验；在存储或传输时是否具备数据包排序及差错校验功能。
   3. 审查厂商提交的文档，查看是否禁止使用私有的、非标准的或业界已知的不安全的密码算法或通信传输协议。
2. 结果判定：
   1. 对业务平台与智能家居终端、其他业务平台之间的敏感信息（敏感信息包括后台系统管理员认证信息、操作系统登录认证信息，网络设备认证信息等）进行加密保护。足为“符合”，其他情况为“不符合”。
   2. 对业务平台与智能家居终端、其他业务平台之间的敏感信息进行完整校验；在存储或传输时具备数据包排序及差错校验功能。足为“符合”，其他情况为“不符合”。
   3. 禁止使用私有的、非标准的或业界已知的不安全的密码算法或通信传输协议。足为“符合”，其他情况为“不符合”。

12.6.4.2 数据访问控制

数据访问控制的检测方法和结果判定如下：

1. 检测方法：
   1. 检查是否支持权限控制功能，在虚拟化系统上对于数据库设置不同的访问策略，尝试用户对该业务系统对应的数据库进行权限以外的相关操作，检查是否可以访问其他未被授权的业务系统数据。
   2. 验证包含敏感信息的文件是否有权限控制，是否只能被相应权限的用户访问。
   3. 上传下载时，验证是否限制用户向上跨目录访问，是否只能访问指定目录下的文件。
2. 结果判定：
   1. 支持权限控制功能，在虚拟化系统上对于数据库设置不同的访问策略，用户对该业务系统对应的数据库进行权限以外的相关操作，不可以访问其他未被授权的业务系统数据。足为“符合”，其他情况为“不符合”。
   2. 包含敏感信息的文件有权限控制，只能被相应权限的用户访问。足为“符合”，其他情况为“不符合”。
   3. 上传下载时，限制用户向上跨目录访问，只能访问指定目录下的文件。足为“符合”，其他情况为“不符合”。

12.6.4.3 数据存储安全

数据存储安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看是否支持分等级的数据加密方法，根据数据密级采用不同的安全存储机制。检查对于重要程度低的数据，是否可以明文存储，保证关键安全信息的保密性。
   2. 审查厂商提交的文档，查看是否支持密钥安全存储；检查是否将密钥存储在加密机或特定代理内部，保证密钥不被泄露。
   3. 审查厂商提交的文档，查看是否支持数据完整性保护，对关键安全信息提供完整性检测机制，关键安全信息损坏和丢失时能够及时发现。检查对用户名、帐号是否采用完整性校验。
   4. 审查厂商提交的文档，查看是否具备完备的数据备份和恢复功能，一旦发生数据丢失或破坏，可以利用备份恢复数据，保证数据在故障发生后不会丢失。
   5. 审查厂商提交的文档，查看是否具备对各类数据和文件进行归档的能力和定期对临时数据及文件自动清理的功能，数据删除后系统内的文件、目录和数据库等资源所在存储空间被释放或重新分配，是否能够完全清除，不可恢复。
   6. 审查厂商提交的文档，查看是否禁止使用私有的、非标准的或业界已知的不安全的密码算法。
2. 结果判定：
   1. 支持分等级的数据加密方法，根据数据密级采用不同的安全存储机制。对于重要程度低的数据，可以明文存储，保证关键数据的保密性。足为“符合”，其他情况为“不符合”。
   2. 支持密钥安全存储；将密钥存储在加密机或特定代理内部，保证密钥不被泄露。足为“符合”，其他情况为“不符合”。
   3. 支持数据完整性保护，对关键安全信息提供完整性检测机制，关键安全信息损坏和丢失时能够及时发现。对用户名、帐号采用完整性校验。足为“符合”，其他情况为“不符合”。
   4. 具备完备的数据备份和恢复功能，一旦发生数据丢失或破坏，可以利用备份恢复数据，保证数据在故障发生后不会丢失。足为“符合”，其他情况为“不符合”。
   5. 具备对各类数据和文件进行归档的能力和定期对临时数据及文件自动清理的功能，数据删除后系统内的文件、目录和数据库等资源所在存储空间被释放或重新分配，能够完全清除，不可恢复。足为“符合”，其他情况为“不符合”。
   6. 禁止使用私有的、非标准的或业界已知的不安全的密码算法。足为“符合”，其他情况为“不符合”。

12.6.5 个人信息安全

个人信息安全的检测方法和结果判定如下：

1. 检测方法：
   1. 查看客户是否能提供GB/T 35273-2017标准中对应项的符合性证明。
2. 结果判定：
   1. 客户提供的证明，符合GB/T 35273 -2017标准中要求。足为“符合”，其他情况为“不符合”。

12.6.6 终端管理安全

终端管理安全的检测方法和结果判定如下：

1. 检测方法：
   1. 审查厂商提交的文档，查看是否支持设备信息安全上报和指令安全下发，验证上报信息和下发指令是否进行完整性校验，是否进行加密处理。
   2. 审查厂商提交的文档，查看是否支持固件安全升级，确保固件升级文件的完整性和机密性，并对固件来源的真实性进行验证。
2. 结果判定：
   1. 支持设备信息安全上报和指令安全下发，上报信息和下发指令进行完整性校验，进行加密处理。足为“符合”，其他情况为“不符合”。
   2. 支持固件安全升级，确保固件升级文件的完整性和机密性，并对固件来源的真实性进行验证。足为“符合”，其他情况为“不符合”。

附 录 A  
（资料性附录）

智能家居典型场景及安全风险分析

### A.1 智能家居典型应用场景

#### A.1.1 家庭娱乐场景

家庭娱乐系统由智能电视、智能投影仪、AR设备、音响等设备组成，通过设备间的联动，为家庭成员提供基于交互的多媒体娱乐环境。

#### A.1.2 设备远程控制

智能家居终端，如智能灯泡、智能电饭煲、智能冰箱等产品，可通过设备app、智能音箱等控制端，实现家庭用户对设备的远程控制，包括设备开启/关闭等功能。

#### A.1.3 家庭安防

智能摄像头、烟感、雾感传感器、智能门磁、智能门锁等家庭安防设备，为家庭用户提供家庭监控、火灾报警等安防功能，保障家庭财产安全。

#### A.1.4 家庭健康

智能心率监测仪、智能血压仪等家庭健康类设备，通过监测用户健康信息并上报云平台的方式，为家庭用户提供实时的安全监护功能。

### A.2 智能家居安全风险

在智能家居安全链条中，存在设备生产商、解决方案提供商、业务运营方、网络运营商、用户等多种角色，所对应的安全利益关注点及安全风险点均不相同。通过对智能家居安全风险分类及利益相关者分析，存在的安全风险如下：

1. 智能家居终端安全风险：智能家居终端存在固件逆向、固件刷写、升级更新校验绕过的风险；设备系统存在密钥硬编码、弱口令等口令风险，以及系统配置不完善、越权访问风险；旁路攻击、物理渗透及芯片攻击的风险。
2. 智能家居网关安全风险：智能家居网关作为面临着与智能家居终端同样的安全风险；网关面临网络接入带来的入侵风险；网络恶意流量带来的安全风险。
3. 网络安全风险：数据传输过程中数据泄露、篡改风险；对于智能家居设备发起的大规模DDoS攻击，使得运营商网络面临网络瘫痪风险；智能家居终端病毒木马在网络环境的传播，为设备、网络及平台带来了攻击风险。
4. 业务应用服务平台安全风险业务应用服务平台存在越权操控、身份伪冒的风险；云平台数据存在被拖库、数据泄露风险；云基础设施存在运维安全风险。

### A.3 智能家居参与方

智能家居涉及七类参与方：设备生产方、服务开发方、应用服务提供方、网络服务提供方、监管方、第三方测评方和用户，各参与方的作用描述和基本关系如图A.1所示。

1. 设备生产方：提供设备的外观模型生产、硬件生产及组装。
2. 服务开发方：为智能家居设备提供业务平台、设备应用及软件开发。
3. 应用服务提供方：为智能设备提供产品规划、业务定义，并提供面向最终用户的业务整体运营。
4. 网络服务提供方：面向最终用户及业务运营方进行网络服务的提供商。
5. 监管方：对智能家居行业具有监督管理职责的国家管理机构。
6. 第三方测评方：独立于智能家居行业买卖双方，以公正、权威的非当事人身份，根据有关法律、标准或合同所进行的智能家居设备或系统的评测方。
7. 用户：智能家居设备业务服务使用方。



图A.1 智能家居角色面及实体的对应关系

参考文献

1. NIST SP800-183 Network of “Things”
2. ISO/IEC 27030 Guidelines for security and privacy in Internet of Things (IoT)
3. ISO/IEC 27033 Information technology -- Security techniques -- Network security
4. ISO/IEC 9798 Information technology -- Security techniques -- Entity authentication
5. ISO/IEC 27034 Information technology -- Security techniques -- Application security