团 体 标 准

立项编号 T/ZSPH—LX201903

《物联网智能家居 安全技术要求》

Security Technical Requirements for Smart Home

xx 年 xx 月 xx 日发布　　xx 年 xx 月 xx 日实施

中关村乐家智慧居住区产业技术联盟 发布

前　言

根据中关村乐家智慧居住区产业技术联盟《关于印发 2019 年度第一批团体标准制修订计划》的通知（中智联【2019】05 号）文件要求，编制组经广泛调查研究，认真总结实践经验，参考有关国外先进标准，并在广泛征求有关科研、设计、施工、生产管理等单位意见的基础上，制定本标准。

本标准共分为 8 章和 2 个附录。主要技术内容是：物联网智能家居系统架构、平台安全、通信安全、智能终端安全等。

本标准由中关村乐家智慧居住区产业技术联盟归口，由全国智能建筑及居住区数字化标准化技术委员会负责解释。执行过程中如有意见或建议，请寄送负责解释单位 （地址：北京市海淀区三里河路 7 号新疆大厦 B 座 12 层 ，邮编：100044 ）

主编单位：全国智能建筑及居住区数字化标准化技术委员会、中外建设信息有限责任公司

参编单位：华为技术有限公司、阿里巴巴、杭州涂鸦信息技术有限公司、小米通讯技术有限公司、杭州奕虎物联科技有限公司、郑州信大捷安信息技术股份有限公司、天津国芯科技有限公司、四川蓝光和骏实业有限公司、上海复旦微电子股份有限公司、大唐微电子技术有限公司、苏州蓝赫朋勃智能科技有限公司、海南普润杰科技有限公司

主要起草人员：张永刚、王钢、尚治宇、樊静静、衣强、刘龙威、黄天宁、李明菊、王英超、陈思刚、梁松涛、张世界、张明旭、王宝东、贾小勇

目　　次

物联网智能家居 安全技术要求

1 范围

本标准规定了物联网智能家居系统架构、平台安全、通信安全、智能终端安全等。

本标准适用于物联网智能家居的设计、制造和应用。

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。

3 术语和定义

下列术语和定义适用于本文件。

3.1

物联网智能家居 Smart home for internet of things

以住宅为平台，融合建筑、网络通信、智能家居设备、服务平台，集系统、服务、管理为一体的高效、舒适、安全、便利、环保的居住环境。

3.2

智能终端 Intelligent terminal

指具备通信功能，可操作和管理的家居设备。

3.3

网关设备 Gateway equipment

智能家居网关为智能硬件设备提供连网和/或设备控制功能，智能家居网关是多种设备的总称，可以是路由器、独立Hub、路由器/Hub混合、中继器、智能家居中控设备等。

3.4

业务云平台 Business cloud platform

对智能终端设备提供注册、管理、控制功能及智能家居服务的平台。

3.5

人机交互终端 Man-machine interactive terminal

指为用户提供交互入口，完成智能家居设备发现、注册过程、管理和控制等功能的终端设备。

4 缩略语

下列缩略语适用于本文件。

ACL 访问控制列表（Access Control List）
AES 高级加密标准(Advanced Encryption Standard)
APP 应用程序（Application）
DDoS 分布式拒绝服务（Distributed Denial of Service)
DES 数据加密标准(Data Encryption Standard)
ECC 错误检查和纠正（Error Correcting Code）
ID 身份识别号（identification）
MD5 单向散列算法(Message-Digest Algorithm 5)
RSA 一种非对称加密算法(Rivest,Shamir,Adleman)
URL 统一资源定位符（Uniform Resource Locator）

5 系统架构

物联网智能家居系统架构如图1所示：

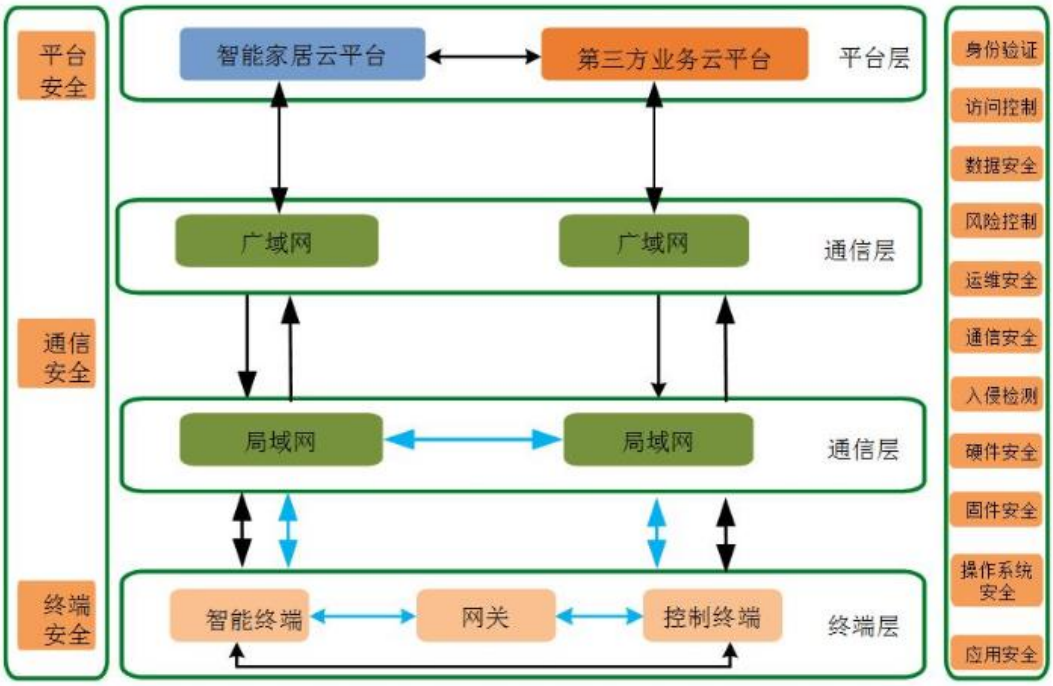

图1 物联网智能家居系统架构

物联网智能家居系统包括平台层、通信层以及终端层三部分构成；

平台层面向智能终端设备提供服务，如设备注册、数据采集、数据监控、安全服务等；

通信层提供网络连接功能，使得智能终端设备通过通信层，实现发现、组网、控制等操作，并可连接到平台层，实现平台对智能终端设备的注册、管理、控制等；

终端层包括智能终端设备、网关设备、人机交互终端设备等，其中智能终端指具

备通信功能，可操控和管理的家居设备，网关指提供智能终端设备局域网网络连接和控制能力的设备，人机交互终端是为用户提供可操作入口、实现对智能设备的管理和控制的终端设备。

物联网智能家居操作系统的安全分为平台安全、通信安全、终端安全，从安全功能角度又可分为硬件安全、固件安全、操作系统安全、应用安全、数据安全、风险控制、运维安全。

注：【大循环】（黑色箭头）大循环即通过广域网完成设备交互，设备间相互通信及互操作需通过网关，经由局域网、广域网、智能家居云平台、第三方业务云平台，再返回至局域网内；【小循环】（蓝色箭头）小循环即局域网内设备交互，设备间相互通信及互操作均通过局域网、网关完成。

6 平台要求

物联网智能家居云平台应满足GB/T 22239-2019《信息安全技术 网络安全等级保护保护基本要求》第三级安全要求中的安全通用要求。

6.1 网络安全

6.1.1 基础设施位置

应保证云平台基础设施位于中国境内。
[GB/T 22239-2019 信息安全技术 网络安全等级保护保护基本要求 8.2.1.1]

6.1.2 网络架构

a) 应保证网络设备的业务处理能力满足业务高峰期要求；
b) 应保证网络各个部分的带宽满足业务高峰期需求；
c) 应提供通讯线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

6.1.3 网络边界

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通讯；
b) 应能够对非授权设备或平台私自联到内部网络的行为进行检查或限制；
c) 应保证物联网智能家居平台网络与外部网络应具备网络隔离措施。

6.1.4 访问控制

a) 应保证接入网络边界网关只开放接入服务相关的端口；
b) 应保证边界安全网关通过 ACL 检测机制对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝异常或非授权数据进出；
c) 应关闭服务器不使用的端口，防止非法访问；
d) 应保证根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制力度到应用级别。

6.1.5 入侵防护

a) 应能够检测接入设备发起的 DDoS 等网络攻击行为；

b) 应保证当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应能够告警并隔离、控制网络威胁；
c) 应保证所使用的操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新；
d) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
e) 应保证易具备对接入平台的终端设备的风险控制，如终端设备上的安全态势分析。

6.1.6 安全审计

a) 应对接入用户的重要安全事件和重要行为进行审计；
b) 应审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
d) 应审计日志应符合相关法律法规要求。

6.2 业务安全

业务安全主要围绕云平台的具体业务功能展开，不要模块包括身份认证鉴权，密钥分发和管理，接入认证和通道加密，用户和设备管理，日志审计和运维监控。而这些模块支撑的业务功能包括用户注册和登录，设备认证、配网和用户绑定、设备和用户交互鉴权、固件升级、云云互联和日志审计等内容。

6.2.1 用户注册和登录

a) 应对用户注册的过程进行有效保护，防止垃圾注册；
b) 应对用户注册或登录涉及的用户密码，进行加密处理后才能传输；
c) 应有效防止用户登录、密码重置、忘记密码等流程进行密码暴力破解，宜通过验证码校验，或对来源客户端、IP、用户等进行阈值设定，超过阈值后进行用户锁定等；
d) 应对所有请求参数进行有效校验，保证会话的完整性。

6.2.2 设备认证、配网和用户绑定

a) 应对设备的身份进行有效验证，需要保证平台内设备的身份信息唯一，不可预测，并拥有足够的长度和复杂度；
b) 应保证用户绑定设备的过程安全可靠，平台需下发对基于用户生成的一次性验证信息，设备配网激活的时候需携带该验证信息，进而进行用户绑定。

6.2.3 用户和设备交互鉴权

设备交互过程，包含了APP与云端交互，以及云端与设备交互，平台的服务包括设备的鉴权，用户的鉴权，设备控制和状态的上报。

所有的交互通信过程，需达到第7章的通信安全的要求。于此同时，还需要如下的保护机制：

a) 应对设备的身份凭证进行有效验证，禁止直接使用设备 ID 等身份索引标识符号直接作为交互的凭证；

b） 应对用户的身份凭证进行有效验证，禁止直接使用用户 ID 等身份索引标识符号直接作为交互的凭证；
c） 应对用户和设备的绑定关系进行严格的校验，防止用户和非其绑定关系的设备进行交互。

6.2.4 固件升级

a） 应保证设备的固件版本准确，在固件升级下发的时候；
b） 应保证固件的完整性和不可抵赖性，对固件进行安全有效的算法验证；
c） 应能够在下发固件的时候，同时下发固件的校验值，宜使用 SM3、SHA256，HMAC 等安全的哈希算法。

6.2.5 云云互联

a） 应保证平台登录接口的安全性，包括确保平台的唯一标识，平台的身份令牌的安全性、不可预测性，并拥有足够的长度和复杂度；
b） 应保证强制的双向的身份校验，宜使用 SM2，ECC，RSA 等安全的非对称算法进行有效身份验证；
c） 应保证平台相互之间应使用精细粒度的访问权限控制，能够根据平台账号分配最小、仅必要的权限，包括对可操控设备，设备类别，区域，用户等的限制。

6.2.6 日志审计

a） 应审计用户的所有操作时间，包括事件的日期、时间、类型、设备标识和结果，对不正常的事件，如频繁大量或不符合的业务参数进行有效记录和告警；
b） 应审计设备的异常状态，包括系统资源的使用情况，设备状态的频繁变化等，进行有效的记录和告警；
c） 应保护审计记录，保证无法删除、修改或覆盖等。

6.3 数据和隐私安全

6.3.1 数据生命周期安全

数据生命周期分为数据采集、数据传输、数据分析、数据存储和数据销毁。在每个阶段都需要特定的安全措施来保护数据安全。

6.3.2 数据安全采集

a） 应保证信息收集主体的所有行为的合法要求，包括信息主体的授权和法律责任的明确；
b） 应保证收集的数据最小化原则，仅采集和保存业务必须的用户个人信息；
c） 应保证用户拥有充分的知情权；
d） 应通过技术手段保障用户的数据访问权、删除权、纠正权和迁移权；
e） 应具有数据敏感度的界定标准，参考国标 GB/T 35273《信息安全技术 个人信息安全规范》相关要求；
f） 应保证数据生产时，根据数据的敏感度进行分类。

6.3.3 数据安全传输

a） 应保证使用安全的加密保护用户数据；
b） 应保证用户数据在不影响业务使用的情况使用脱敏后传输；

c） 应符合第 7 章的通信安全要求，保障通讯安全；
d） 应保证安全可靠的密钥管理方式，采取完整的密钥全生命周期的管理，包括创建、激活、禁用、转换、分发、备份、销毁等，同时基于密钥的数据加密存储；
e） 应保证使用动态密钥或设备唯一密钥，保障设备安全；
f） 应保证数据完整性校验，对数据包的所有内容进行签名，同时包含硬件的授权信息和唯一识别 ID 等。

6.3.4 数据安全使用

a） 应禁止未授权访问和非法使用使用用户个人信息；
b） 应保证敏感数据必须具备权限控制。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。

6.3.5 数据安全存储

a） 应保证数据隔离，对敏感数据进行集中地分布式存储，统一监控管理，通过 VPC 隔离；
b） 应对文件数据采用加密技术实现文件的存储保密性；
c） 应对数据库采用加密技术实现数据的存储保密性；
d） 应对关键信息，如隐私信息，除了保证存储保密性，还需要在此之前完成脱敏；
e） 应保证数据存储在中国境内；
f） 应采用分布式架构，所有业务服务器同时部署于同城不同中心的三个机房，数据库等数据存储服务采用多副本模式(最少保证二个实时副本)，并进行实时数据备份。

6.3.6 数据安全销毁

a） 应能够提供手段协助清除因数据在不同存储设备间迁移、业务终止、自然灾害、合同终止等遗留的数据，对日志的留存期限应符合国家有关规定；
b） 应提供手段清除数据的所有副本。

7 通信要求

物联网智能家居与业务平台之间通信会话应符合以下要求：
a） 通信会话建立前应有安全的接入认证机制；
b） 传输敏感数据时的加密密钥禁止硬编码在代码中；
c） 关闭不必要的通信端口，监听端口应先在合理的范围；
d） 通信会话应支持加密、完整性保护及防重放攻击，建议使用 TLS/DTLS 安全通信协议；
e） 禁止使用 SSL2.0、SSL3.0 协议；
f） 通信会话标识应使用安全随机数算法生成；
g） 会话服务端应对客户端的请求进行合法性校验，包括校验会话标识、及会话标识是否与用户 IP 匹配；
h） 禁止在 URL、错误信息或日志中暴露会话标识符；
i） 所有登录后才能访问的界面都应提供主动退出选项，当用户退出时，服务器端应清除该用户的会话信息；
j） 应设置会话超时机制，在超时过后必须要清除该会话信息。

8 智能终端要求

8.1. 终端及网关安全要求

8.1.1 智能终端设备安全分级

智能终端设备依据自身在身份认证、硬件、操作系统、固件等安全能力，依次划分三个安全等级，安全能力从低到高分别为：LeveL1、Level2、Level3。满足不同应用场景的安全需求。依次对不同安全等级的智能终端设备提出安全需求。

a) Level1 级智能终端应可在使用密钥时可以进行软件级隔离并保障一定的安全性并可以抵抗大规模软件攻击，应支持如软件沙箱、白盒加密等技术，并满足以下基本要求：
   ——具备设备认证能力，实现终端设备身份认证；
   ——具备硬件安全能力，应提供最小外部接口；
   ——具备操作系统安全，应能抵御通用软件外部攻击能力。
b) Level2 级智能终端应可在使用密钥时可以进行逻辑级隔离并应可以抵御大规模软件攻击、可在操作系统层被攻破的情况下仍然保障密钥的安全性，应支持如可信执行环境、安全 MCU 芯片等技术，在满足 level1 级安全能力要求基础上，应满足以下基本要求：
   ——具备设备认证能力，实现基于数据证书的身份认证；
   ——具备硬件安全能力，应提供防止简单物理攻击的能力；
   ——具备操作系统安全，应能预防通用外部攻击能力。
c) Level3 级智能终端应可支持物理隔离安全性、芯片级防篡改保护机制并具备可抵御芯片级攻击能力，可在物理设备层被攻破的情况下仍然保障密钥的安全性，应支持安全芯片或同等安全能力的安全单元。在满足 level2 级安全能力要求基础上，应满足以下基本要求：
   ——具备独立的密码安全芯片，为系统提供独立的安全秘密服务；
   ——具备硬件与平台双向认证能力，实现基于硬件的数字证书机制，宜采用国产密码算法；
   ——具备硬件应具备防止外部物理攻击能力；
   ——具备操作系统安全，应采用可信计算等技术，保证系统安全，内部程序采用白名单机制。

8.1.2 身份认证技术要求

Level1级智能终端应满足以下安全要求：

a) 智能家居平台应认证智能家居终端设备及身份的合法性，智能家居终端也宜验证智能家居平台的合法性，终端与智能家居平台进行身份认证时应至少支持挑战应对模式和时间戳模式；
b) 终端应具有唯一的终端身份识别信息，身份识别信息应不可篡改、不可预测、不可伪造、具备全球唯一性且由智能家居平台进行统一管理；
c) 终端身份识别信息应与终端设备信息进行关联，如设备厂商代码、设备型号代码、唯一标识代码、身份识别服务规范版本号等，具体身份识别信息格式应符合 GB/T 37743-2019 《信息技术 智能设备操作系统身份识别服务接口》中相关内容，详见附录 B；

d) 终端应支持密钥的生成、分发、存储、更新等密钥管理功能。根密钥应至少支持国产密码算法，可选支持国际算法。

1）非对称密钥：

——SM2；

——RSA 2048bit

——ECC 256bit(prime256v1 曲线)

2）对称密钥：

——SM1/SM4；

——AES 128bit；

——AES 192bit；

——AES 256bit；

——3DES 112bit；

——3DES 168bit。

3）摘要算法：

——SM3；

——MD5；

——SHA1；

——SHA256；

Level2、3 级终端应在满足 Level1 的要求基础上，满足以下安全要求：

e) 应通过出厂预置密钥、产线烧录密钥、密钥个人化协商等方式，使每个设备具有唯一的设备根密钥，且设备根密钥与终端身份识别信息一一绑定。终端认证过程中禁止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；

f) 智能终端设备应支持在生产产线为身份识别模块烧录身份识别信息及设备根密钥。智能家居平台应可对身份识别信息的进行分发、加密及认证。智能终端设备生产产线应具备对身份识别模块进行身份识别信息及密钥的烧录、返回烧录回执、产线激活、信息校验等功能。

8.1.3 硬件安全

Level1级智能终端应满足以下安全要求：

a) 对于具有控制台接口的设备，需配置用户名、口令等方式进行认证授权，禁止直接登录；

b) 对具备 USB 接口的设备，应默认关闭 USB 调试接口功能，或者增加调试接口验证功能或禁用，默认禁用/删除该接口的管理、调试功能；

c) 不再使用的物理接口应移除或禁用。

Level2 级终端应在满足 Level1 的要求基础上，满足以下安全要求：

d） 安全能力为Level2级的智能终端设备应支持安全隔离功能，提供可信执行环境；

e） 应具备固件芯片的物理写入保护的功能，防止固件被恶意篡改。

Level3 级终端应在满足 Level2 的要求基础上，满足以下安全要求：

f） 安全能力为Level3级的智能终端设备应支持硬件安全隔离功能。

8.1.4 终端设备操作系统安全

Level1级智能终端应满足以下安全要求：

a) 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；
b) 应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，并进行定期的检查校验；
c) 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；
d) 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；
e) 智能家居终端的操作系应能够实现用户、进程空间和文件系统的沙箱隔离；
f) 系统应具有有防回滚策略，防止系统被恶意降级；
g) 应禁止开放系统根权限或超级管理员权限；
h) 系统应减少开放网络服务，比如减少开放端口 23 的 telnent，端口 80 的 http 等；
i) 对于任何的外界输入，系统应做充分的参数检查，以防系统根权限被获取；
j) 应禁止预留任何的未公开帐号，所有帐号应可被系统管理，并在资料中提供所有帐号及管理操作说明；

Level2 级终端应在满足 Level1 的要求基础上，满足以下安全要求：

k) 系统在应用安装时应获得用户授权，未知来源或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；
l) 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；
m) 应禁止存在绕过正常认证机制直接进入到系统的隐秘通道，包括不限于：组合键、特殊敲击、连接特定接口、使用特定客户端、使用特殊 URL。

Level3 级终端应在满足 Level2 的要求基础上，满足以下安全要求：

n） 系统应包含网络流量的安全监控机制，能发现并阻断针对恶意钓鱼网站的访问；
o） 系统应包含系统运行空间的安全监控机制，包括针对进程、服务、开放端口等核心要素的监控，能及时发现恶意程序并强制关闭删除；
p） 操作系统应支持检查上报系统文件的完整性。操作系统应定期扫描系统中已有的系统核心文件，计算文件的摘要值并上报智能家居平台，及时发现并阻止未知恶意程序篡改系统核心文件；
q） 操作系统应支持对系统进程的动态行为采集。动态行为采集应监控系统进程在运行过程中的操作，比如网络访问、设备访问、文件访问、打开设备驱动、进程间通信等。及时阻止在基准行为规则之外的的恶意操作和恶意程序运行。

8.1.5 固件安全

Level1级智能终端应满足以下安全要求：

a) 终端固件及对固件的任何改动都应经过严格的流程控制和认证，以保证固件中不含隐藏的非法功能；

Level2、3 级终端应在满足 Level1 的要求基础上，满足以下安全要求：

b) 固件升级时，应对新版固件进行验签，保证新版固件的合法性；
c) 终端上电时应对固件做真实性、完整性校验，确保固件未被非法篡改。

8.2 人机交互终端安全要求

8.2.1 人机交互终端系统要求

8.2.1.1 内部存储

a) 系统私有目录本地部分存放的配置文件等信息，通过安全的加密方式保存，包括严格的读写执行权限设置；
b) 系统数据库不应存储用户相关的敏感信息；
c) 在人机交互终端本地不存储所有智能家居设备的 token 等涉及设备安全的信息；
d) 在未授权拿到 token 之前，人机交互终不应主动获取智能家居设备的信息；
e) 人机交互终系统配置文件不应出现敏感信息。

8.2.1.2 系统日志

a） 人机交互终系统不应打印和存放任何交互 logcat 或日志文件；
b） 人机交互终系统不应打印和存放任何从智能家居设备获取的信息的日志文件。

8.2.1.3 密钥链数据

不应硬编码重要的密钥。采用自主研发的安全算法保存密钥。

8.2.1.4 内存数据

重要操作时候，用户数据不应存入内存。

8.2.1.5 组件安全

a) 针对四大组件，Activity、Broadcast Receiver、Service、Content Provider，严格限制组件的使用权限和访问权限，同时针对对外开发的组件，进行严格的权限和输入校验；
b) 针对 WebView，保持 SDK 较高版本，针对 URL 域名和 file 访问权限进行严格控制。

8.2.1.6 代码安全

a) 签名应校验客户端完整性；
b) 对核心业务代码应进行混淆；
c) 应通过对调试进程的监听，增加反调试功能。

8.2.2 人机交互终端应用要求

a) 应用程序禁止存在病毒、木马、恶意脚本/代码，以及发送恶意广告、吸费、恶意消耗流量的行为；
b) 软件安装包应进行完整性保护并确保完整性校验流程安全可靠；
c) 应用程序执行从文件中读取的命令或调用外部脚本时要严格限制该文件的脚本的修改权限，防止注入攻击；
d) 应用程序必须设置对外交互组件的访问权限；
e) 禁止口令输入组件提供拷出功能；

f) 必须对涉及现实或虚拟货币应用的口令输入框实现安全输入机制；
g) 涉及现实或虚拟货币的应用必须实现 root 检测及风险控制；
h) 禁止应用提供设备权限破解功能；
i) 应用程序禁止缓存敏感信息；
j) 应用程序只申请业务必要的权限；
k) 应用程序应实现自动检测更新机制；
l) 应用的保持登录选项，应能够让用户自主选择和取消；
m) 应对涉及现实或虚拟货币操作的应用提供会话保护机制；
n) 应对涉及现实或虚拟货币交易操作提供重认证；
o) 对于每一个需要授权访问的 Web 请求,必须核实用户的会话标识是否合法、用户是否被授权执行这个操作；
p) 对 Web 用户的最终认证处理过程必须放到服务器进行；
q) 在 Web 服务器端对所有来自不可信数据源的数据进行校验，拒绝任何没有通过校验的数据。若输出到 Web 客户端的数据来自不可信的数据源，则须对该数据进行相应的编码或转义；
r) Web 应用程序的会话标识必须具备随机性、唯一性；身份验证成功后，必须更换会话标识；
s) 通过 Web 上传文件时，必须在服务器端采用白名单方式对上传到 Web 内容目录下的文件类型进行严格的限制。

附 录 A

智能设备身份识别信息应采用以下信息格式：

共24个十六进制数字字符，分为5个字段。从左到右，只有在前面的字段（上位字段）完成所有各字符取值后，才能对紧随其后的字段（下位字段）中各字符赋值。对于同一个上位字段值，其下位字段的取值应唯一，格式见图1。

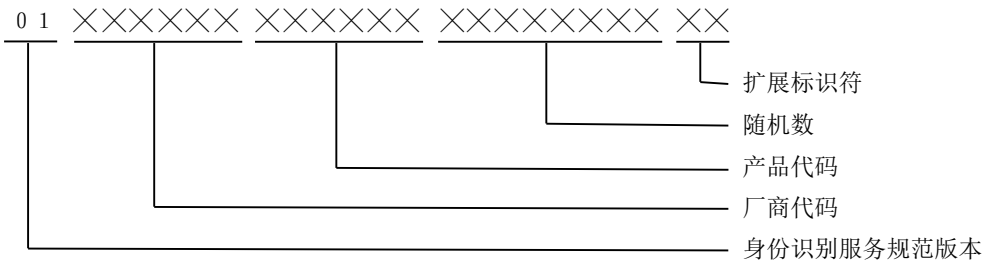

图1 信息格式

其中：

a) 身份识别服务规范版本：2 位，本标准为 01；

b) 厂商代码：6 位；

c) 产品代码：6 位；

d) 随机数：8 位；

e) 扩展标识符：2 位。

附　录　B

智能家居系统安全云平台包括认证系统、密钥系统、接入系统、管理系统、审计系统和运维系统，可实现不同智能家居厂商接入和数据交互，并具有以下功能：

——身份认证鉴权

——密钥分发和管理

——接入认证和通道加密

——用户和设备管理

——日志审计、行为审计

——运维监控

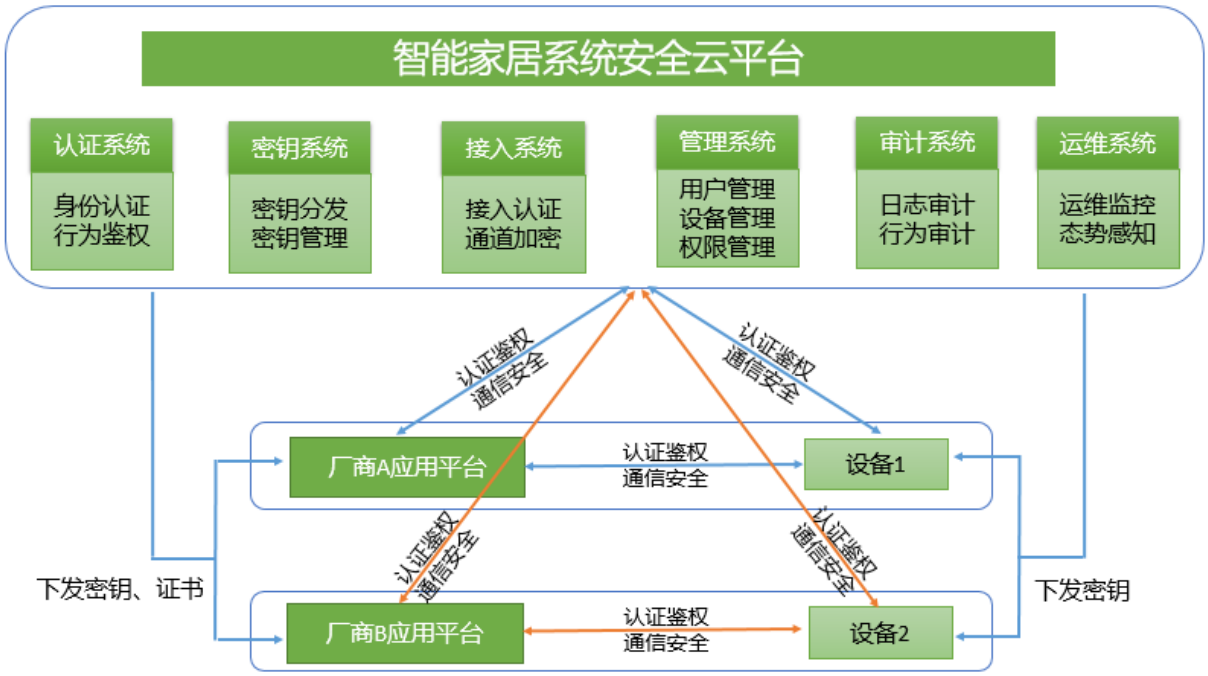

图2　　智能家居系统安全云平台