ICS 号
中国标准文献分类号

团　　体　　标　　准

团体标准编号

《长租公寓（含公租房）智能化技术》

Intelligent technology of long-term rental apartment（including public rental housing）

（征求意见稿）

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

目　　次

前　言

本标准按照 GB/T 1.1-2020 给出的规则起草。

本标准由中关村乐家智慧居住区产业技术联盟提出并归口。

本标准起草单位：

本标准主要起草人：

长租公寓（含公租房）智能化技术

1 范围

本标准规定了长租公寓（含公租房）智能化技术管理平台总体架构、基础设施要求、平台功能要求、应用层技术要求、安全要求等。

本标准适用于长租公寓（含公租房）智能化技术建设应用，设备管理、数据保护等。

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。

GB 14287.1 电气火灾监控系统 第1部分：电气火灾监控设备

GB 14287.2 电气火灾监控系统 第2部分：剩余电流式电气火灾

GB 14287.3 电气火灾监控系统 第3部分：测温式电气火灾监控探测器

GB 17859 计算机信息系统安全保护等级划分准则

GB 20517 独立式感烟火灾探测报警器

GB 21556-2008 锁具安全通用技术条件

GB/T 22080 信息技术 安全技术 信息安全管理体系要求

GB/T 28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 28847.3 建筑自动化和控制系统 第3部分:功能

GB/T 30146 公共安全 业务连续性管理体系要求

GB/T 35273 信息安全技术个人信息安全规范

GB 50348 安全防范工程技术标准

GB 50395 视频安防监控系统工程设计规范

GA/T 72 楼寓对讲电控安全门通用技术条件

GA 374-2019 电子防盗锁

GA 701-2007 指纹防盗锁通用技术条件

ISO/IEC 27001 信息技术 安全技术 信息安全管理体系 要求（Information technology—Security techniques—Information security management systems—Requirements）

ISO/IEC 27018 信息技术 安全技术 个人可识别信息(PII)保护工作守则（Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors）

3 术语和定义

下列术语和定义适用于本文件。

3.1

长租公寓

新建、改造、购买或租赁整幢楼宇或分散设置的房屋，并将其出租给公司、家庭、个人用于居住的公寓。

[注：参考T/SZZX-006-2019，2.1.1]

3.2

SM2算法　SM2 algorithm

一种非对称密码算法，其密钥长度为256位。

3.3

SM3算法　SM3 algorithm

一种密码杂凑算法，其输出长度为256位。

3.4

SM4算法　SM4 algorithm

一种分组密码算法，其分组长度和密钥长度均为128位。

3.5

智能消防监测预警装置　Intelligent fire monitoring and early warning device

指电气火灾监控探测器和独立式感烟火灾探测报警器。

4　缩略语

下列缩略语适用于本文件。

AES　高级加密标准（Advanced Encryption Standard）

AI　人工智能（Artificial Intelligence）

API　应用程序接口（Application Programming Interface）

APP　应用软件（Application）

B/S　浏览器/服务器模式（Browser/Server）

CDMA　码分多址（Code Division Multiple Access）

GPRS　通用分组无线服务技术（General Packet Radio Service）

IP　网际协议（Internet Protocol）

KMS　密钥管理服务（Key Management Service）

LoRa 长距离无线电（Long Range）

LwM2M　轻量化物联网（Lightweight Machine to Machine）

MPU　内存保护单元（Memory Protection Unit）

MQTT　消息队列遥测传输（Message Queuing Telemetry Transport）

NB-IoT　窄带物联网（Narrow Band Internet of Things）

NFC　近场通信（Near Field Communication）

PSTN　公共交换电话网络（Public Switched Telephone Network）

RCC　限域通信（Range Controlled Communication）

SDK　软件开发工具包（Software Development Kit）

SE　安全模块（Security Element）

SIM　用户识别模块（Subscriber Identity Module）

TCP　传输控制协议（Transmission Control Protocol）

TDES　三重数据加密标准（Triple Data Encryption Standard）

TLS/HTTPS　安全传输层协议/超文本传输安全协议（Transport Layer Security/Hyper Text Transfer Protocol over SecureSocket Layer）

UDP　用户数据报协议（User Datagram Protocol）

Wi-Fi 无线保真（Wireless Fidelity）

5　总体架构

5.1　系统组成

长租公寓（含公租房）智能化系统由物联设备、管理平台、终端应用及三大模块组成，并且保留第三方的扩展对接能力，见图1所示。并应符合下列要求：

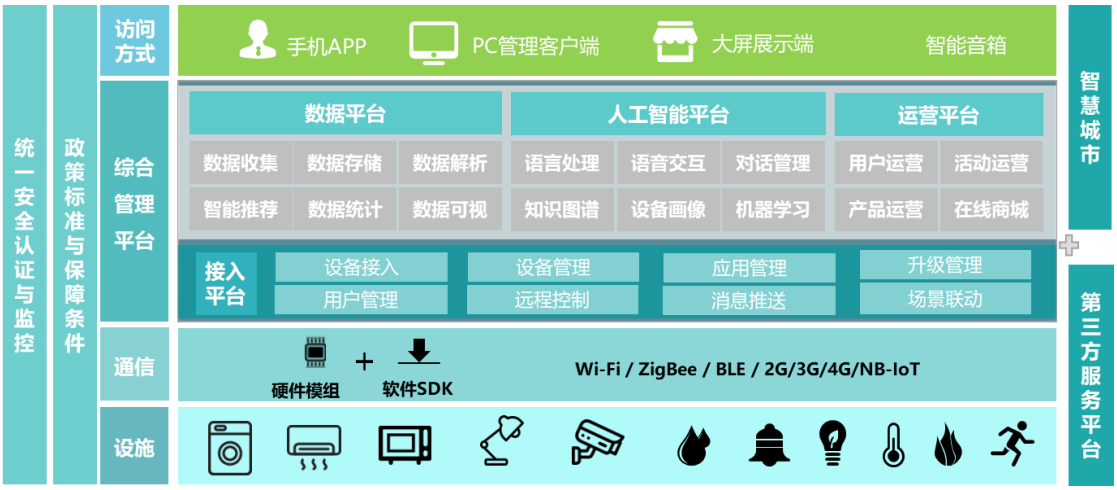

图1　系统框架图

a)　物联设备：包括但不限于智能门禁、火灾消防、智能表、智能家居、视频监控、可视对讲等子系统，通过近场或远程通信能力的硬件模组，实现设备接入、状态、控制和数据采集功能，并能支撑上层应用的设备控制和管理、人员分析和管理、运营管理和数据分析；

b)　管理平台：面向公寓、设备、租户、公寓所有者、设备供应商、运营商等长租公寓（含公租房）运营对象，通过物联网技术和大数据分析技术应用，对各方运行数据进行管理、采集和分析，实现公寓、设备、租户全生命周期管理功能。管理平台包括设备管理平台、软件管理平台，并应符合下列要求：

1)　设备管理平台：封装长租公寓（含公租房）常用设备的接入接口，并应实现电表、水表、智能锁、烟感等物联设备注册入网管理、设备管控、设备运行数据采集等功能；

2)　软件管理平台：包括数据管理系统、人工智能系统、运营管理系统，并定义开放 API 接口，使运营管理方根据需求自定义应用层功能。软件管理平台应与智慧城市（包括但不限于政务、物流、交通等）、第三方服务（包括但不限于水、电、暖、物业、周边等）进行对接融合。软件管理平台应设计有私有化本地部署方案。

c)　终端应用：通过站点、APP、微信、信息牌等终端入口，提供服务给租户、房东、运营商，服务功能应包括但不限于房源管理、设备管理、租户管理、租务管理、财务管理、统计分析、安防管理等。

5.2　网络架构

长租公寓（含公租房）智能化系统宜采用三层网络架构，从下到上依次是设备网络层、远传通讯层、主站应用层。并应符合下列要求：

a)　设备网络层：由智能传感器、物联网表以及终端采集设备等组成，智能传感器和物联网表应通过有线或无线与终端采集设备连接，有线包括 modbus、RS485 等，无线包括 NB-IoT、LoRa、Wi-Fi 等；

b) 远传通讯层：由 GPRS/CDMA/4G/5G、PSTN、企业光纤城际网络、城市广域网络等组成，应根据实际情况选择最实用和最经济的组网方式；
c) 主站系统层：由应用系统及其环境组成，环境内网应采用双网冗余运行，各系统间应有防火墙阻止隔离黑客和病毒攻击，保障系统的安全运行环境。

5.3 系统设计要求

长租公寓（含公租房）智能化服务平台设计宜采用B/S架构模式，平台软件应采用JavaEE企业平台架构搭建，采用多层的分布式应用模型、组件再用、一致化的安全模型及灵活的事务控制，使系统具有更好的移植性，以适应用信息采集系统应用环境复杂、业务规则多变、信息发布的需要，以及系统将来的扩展的需要。

长租公寓（含公租房）智能化系统设计宜采用多层结构体系和分布式模式，满足长租公寓（含公租房）智能化业务技术创新、管理创新、服务创新、文化创新、体制创新这样一个不断以租户为中心的不断创新、扩展、规范的业务要求。

6 基础设施要求

6.1 智能门锁管理

6.1.1 基本要求

智能门锁由面板、把手、锁体/锁芯、控制电路组成，安装在长租公寓和公租房入户门或房门上，仅有合法授权的住户方能开启。

6.1.2 主要功能及技术要求

智能门锁的主要功能应符合下列要求：

a) 应符合 GA 374、GB 21556、GA 701 等标准要求；
b) 应具有近场或远程通信能力，可通过如 Bluetooth、Zigbee、Wi-Fi 等短距离通信方式，或 2G/3G/4G/5G/NB-IoT 等远距离通信方式和远端云服务平台之间通信；
c) 应具有以下一种或多种开锁凭据：密码、人体生物特征、NFC、RCC、身份证、居民身份证网上功能凭证等,在联网和非联网状态下均应能下发开锁凭据，且开锁凭据有效期可维持一年以上；
d) 应具有防撬报警、低电预警、连续多次密码输入失败（最多连续 5 次）报警等异常检测功能，并将异常上报服务器；
e) 应具有开门记录存储和上报等记录功能，并将记录上报服务器；
f) 智能门锁设备在断网时应能够自动重连，无需再重新手动配置。

6.2 火灾消防管理

6.2.1 基本要求

智能消防监测预警装置应能够监测引发电气火灾的剩余电流、温度等参数的变化，预防电气火灾发生，应能够智能判断火灾发生时产生的烟雾参数，监测数值超限并发出报警，报警方式除了本地发出高分贝声音和光的提示外，还可将报警信息发送到手机 APP 和电脑端，社区管理平台收到报警信息进行处置，实现无遗漏告警。

6.2.2 主要功能及技术要求

智能消防装置的主要功能应符合下列要求：

a) 应符合 GB 20517、GB 14287.1、GB 14287.2、GB 14287.3 等标准要求；
b) 火灾监控探测器的监控报警信号，应在 20s 内发出声、光报警信号后、指示报警部位、显示报警时间等，并予以保持直至监控平台进行复位操作；
c) 当监控设备发生故障时，应能在 60s 内发出与监控报警信号有明显区别的声、光故障信号；
d) 火灾监控探测器在封闭的配电箱内，在报警条件下，其音响器件在正前方 1m 处的声压级(A 计权)应大于 70dB，小于 115dB；
e) 应支持对本机及所配接的探测器进行功能自行检查，应能手动蜂鸣器、指示灯、显示器的工作状态；
f) 宜采用 NB-IoT、2G、4G、5G 等无线通信技术，部署方便、通讯距离远，传输能力强，产品功耗降低的技术；
g) 电池供电的智能消防监测装置，电池的容量应能保证报警器正常工作不少于 3 年；
h) 感烟火灾探测报警器应具有防拆、防盗及时提醒功能。

6.3 智能表类管理

6.3.1 基本要求

智能表类包括但不限于水表、燃气表、电表等，应支持将基表的机械读数转化为电子读数，并支持远程无线抄读管理，方便管理平台进行结算。应采用超低功耗的微电子技术，在单电池供电的情况下可确保多年免维护的使用寿命。

6.3.2 主要功能及技术要求

智能表类的主要功能应符合下列要求：
a) 应根据周期间隔采集用户数据，并保存为冻结数据，24 小时采集数据，本地冻结存储 30 天以上抄表定时点的数据，有利于后台数据的用量统计与趋势分析；
b) 应具有自动网络连接、离散上报冻结数据、数据加密、即时触发读数上报、数据补报、电池低电压报警等功能，下行可通过平台下发参数设置、开关阀等指令；
c) 应提供集成阀门控制电路，支持阀门开、关功能，触发上报和定时上报期间可接收开关阀指令，实现远程付费管理等；
d) 应具备磁干扰检测功能，遇到磁攻击提供及时报警；
e) 应具备进行自动校时，保证表端采集和数据上报时间准确性，为准确计费缴费提供保证；
f) 应支持通过平台远程升级实现智能表具远端维护功能。

6.4 智能家居管理

6.4.1 基本要求

智能家居包括但不限于信息设备、通信设备、智慧电视、AI 音箱等家用电器、照明设备等产品，可通过各种无线/有线方式连接，应具有数据采集、联动控制和网络服务功能，可实现居住品质提升、家居设备的自动化和智能化、提供一个安全、高效、舒适、便利的家居环境。

6.4.2 主要功能及技术要求

智能家居的主要功能应符合下列要求：
a) 应具有智能家居 APP，用于辅助完成智能家居设备的设备发现、注册过程，并可以

管理和控制智能家居设备；

b) 宜采用 Wi-Fi、NB-IoT、4G/5G、Bluetooth、Zigbee 等先进无线通信技术，宜采用 TCP、UDP、LwM2M、MQTT 等通信协议；

c) 应可以通过 APP 或智能网关完成设备注册和接入；

d) 应支持家居联动控制；

e) 家居环境变化时，应通知到租户，尤其是针对告警类型的属性变化；

f) 为保证数据传输安全，应采用加密通信技术；

g) 智能家居设备应支持在线升级功能。

6.5 视频监控管理

6.5.1 基本要求

视频监控摄像机应安装于长租公寓/公租房主要出入口、机动车出入口、停车场（库）出入口、电梯轿厢、主要通道及每幢公寓楼/住宅楼单元出入口等部位，公共区域（含正门外）不应出现监控盲区，在面积较大的公共区域应安装具有转动和变焦的摄像机。

6.5.2 主要功能及技术要求

视频监控系统的主要功能应符合下列要求：

a) 应符合 GB 50348、GB 50395 的相关要求；

b) 应支持实时视频监控上墙、录像回放、远程监控、多路画面分割、视频轮巡和云台控制等功能；

c) 应具有视频移动侦测功能，宜具有人脸识别、行为识别、目标跟踪、车牌识别等功能；

d) 用于周界防范的摄像机，应具备夜间报警灯光联动的功能；

e) 应具有时间、日期的字符叠加、记录和调整功能，字符叠加应不影响对图像的监视和记录效果，字符时间与标准时间的误差应在±30s 以内；

f) 视频监控数据应能存储 30 天以上；

g) 应具有视频联网接口，联网接口应符合 GB/T 28181-2016 的相关要求；

h) 应支持自动检测视频信号缺失、异常，视频图像的遮挡和转动实时告警；告警发生时，告警消息能够分级发送。

6.6 人脸识别管理

6.6.1 基本要求

人脸抓拍单元应安装在长租公寓出入口、公共通道等区域，获取并记录进入小区和公寓/住宅楼内的人员图像，提供实时比对布控、黑名单报警、历史数据查询、轨迹分析等服务。同时，将前端采集数据接入监管部门指定平台。

6.6.2 主要功能及技术要求

人脸识别系统的主要功能应符合下列要求：

a) 应支持人脸抓拍功能，能够对经过设定区域的行人进行人脸检测和人脸跟踪抓拍，人脸检出率应不低于 99%，应支持检出两眼瞳距 30 像素点以上的人脸图片，宜支持 20 像素点；同时检测不少于 30 张人脸；

b) 应支持单场景同时检出多张人脸图片，并支持从人脸轨迹中筛选出一张最优的人脸图像作为该行人的抓拍图像；

c） 应支持对动态抓拍库、静态名单库的人脸查询；
d） 应支持按照时间地点以及结构化信息查询；
e） 应支持地图选点查询；
f） 应支持利用已有人脸照片（前端人脸抓拍机抓拍的人脸照片或治安监控截取的清晰人脸图片），在静态人脸特征数据库中检索出与其最相似的人员；
g） 系统可对前端人脸抓拍机抓拍的人脸与布控库进行实时比对，当抓拍人脸与布控库的人脸相似度达到设定报警阀值时，系统应进行实时自动报警。

6.7 可视对讲管理

6.7.1 基本要求

长租公寓/公租房住宅楼栋（单元）口应安装访客可视对讲主机和电控防盗门；在住宅内应安装可视对讲分机；地下车库进入电梯厅或消防楼梯的通道口，应安装可视对讲，电磁锁电源应与安防管理中心或监控中心联动，确保火警时电磁锁处于开启状态。

6.7.2 主要功能及技术要求

可视对讲系统的主要功能应符合下列要求：
a） 应符合 GA/T 72 的相关要求；
b） 对讲主机应具有图片抓拍功能，采用基于 TCP/IP 联网技术的系统，在中心应具有图片存储功能；
c） 对讲主机应能正确选呼任一对讲分机，并能听到回铃声；
d） 对讲主机选呼后，应能实现小区出入口与住户、楼栋口与住户间对讲或可视对讲，语音（图像）清晰；
e） 对讲分机应能实现电控开锁；
f） 对讲主机可使用密码、钥匙或感应卡等方式开启访客（可视）对讲电控防盗门锁；
g） 可视对讲系统的报警联网系统功能应符合 GB 50348 有关规定。

6.8 门禁管理

6.8.1 基本要求

公寓、小区楼栋主要出入口应安装门禁系统，租客入户门宜安装智能门禁设备，对人员通行权限进行管理，包括钥匙、IC卡、CPU卡、RCC SIM卡、手机APP、蓝牙、人脸识别、指纹、应急密码等多种门禁方式，只有经过授权的人才能进入受控区域门组，如权限合法则开门。

6.8.2 主要功能及技术要求

门禁管理系统的主要功能应符合下列要求：
a） 应支持多种开门方式，包括但不限于人脸、CPU 卡、二维码、蓝牙、NFC、RCC、身份证、身份证网上副本等，用户可任意选择一种作为其开门使用；
b） IC 卡、CPU 卡信息在存储、传输、认证过程中应安全可靠，卡片不可复制；
c） 应具备人证识别比对功能，通过用户的身份证照片与摄像头拍摄的本人照片进行 1：1 的人脸比对，保障登记的证件信息与本人一致；
d） 应能针对用户的门禁权限进行开卡、挂失、注销操作，并实时生效；
e） 应根据不同的用户类型区分不同有效期，业主的门禁长期有效，租客如果合同到期或居住证到期，门禁自动失效；

f） 应需实时、准确记录所有门禁的出入信息，包括人员、出入时间、地点、开门方式，并记录用户开门时的照片等信息；
g） 应具有操作记录日志功能，对核心功能模块数据的修改、删除、查询、增加进行记录、查询；
h） 宜支持视频语音对讲功能，可呼叫中心管理机与室内机；支持远程视频预览；
i） 宜支持权限信息的增删改查，判定权限信息有效性，并根据其进行人员通行管理；
j） 应具备网络连接功能，支持通过有线或无线方式接入；
k） 应具备系统时间同步服务功能，校准次数一天不少于一次；
l） 应具备语音播报功能，对无权限、卡过期的刷卡行为进行语音播报提醒。

6.9 居住人员管理

6.9.1 基本要求

长租公寓/公租房应设身份验证管理系统对租客进行实名制入证，系统应配置人证核验设备、人证访客机、采集一体机、业务自助办理机、身份证阅读器、电脑、USB高清摄像头等设备，安置于公寓大厅、小区管理中心或出入口岗亭。应支持对人员进行身份证信息的采集、查询、比对，以及建立长租公寓/公租房基本信息库。

6.9.2 主要功能及技术要求

居住人员管理系统的主要功能应符合下列要求：
a） 应支持人员身份核验及信息登记，通过 1:1 比对身份证内照片与采集的人脸照片，核验人员身份，并在长租公寓/公租房管理平台录入身份信息、人脸、指纹等信息；
b） 应支持需登记人员的住房信息标准地址录入；
c） 应支持公租房小区访客信息登记，在小区入口部署人证访客机，人证核验比对通过后由小区保安或物业人员与被防人员核实 ，确认后发放访客临时卡进入小区，进入设定的门禁点；
d） 对已完成登记人员进行权限配置，开放公寓/小区入口、所住单元楼/公寓楼等固定的门禁权限，门禁权限由公寓/小区管理人员控制。

7 平台功能要求

7.1 接入平台

7.1.1 基本要求

接入平台应提供统一的接入服务，能够控制前述基础设施，并能够获取和设置基础设施（下称设备）的状态和属性，包括但不限于查看视频监控系统的视频数据、开启关闭智能楼宇对讲、获取智能水电表的读数、下发智能门锁开锁凭据（如密码等）。

7.1.2 主要功能及技术要求

接入平台的主要功能应符合下列要求：
a） 应能提供局域网或互联网通信服务，设备可通过网线、Wi-Fi、LoRa、蓝牙、2G/3G/4G/5G、NB-IoT 等一种或多种通信方式接入平台；
b） 应保证设备与所有者的唯一对应关系，通过权限控制来保护所有者对设备的所有权和控制权；
c） 应能对设备进行控制、操作或状态读取；

d) 应存储设备的状态、属性、操作记录，或其他重要信息，并定期更新；
e) 应能支持设备的远程升级能力；
f) 应能监控设备的状态，当出现状态异常，或设备报警时，应能及时预警，并存储异常和报警记录；
g) 应保证服务的高可用性，达到 99%可用。

7.2 数据和人工智能平台

7.2.1 基本要求

平台可对接入平台的运行数据、设备的运行日志、异常和事件流进行收集、存储和挖掘，并通过聚合的方式对数据进行二次加工，得出可视化、可分析的大数据信息。

7.2.2 主要功能及技术要求

数据和人工智能平台的主要功能应符合下列要求：
a) 应能整合各个业务系统数据，数据源来自接入平台的设备属性、操作行为、运行日志、设备事件、设备异常等，并做存储；
b) 应能将存储的数据以一定的组织形式，如时间、来源等方式进行分类归档；
c) 应能通过云计算引擎对数据进行抽取、转换、加载面向各个业务应用，加工基础公共层，产出应用数据；
d) 应能通过可视化方式汇总和展示各类数据报表，为决策提供支持，构建完善的经营分析模型；
e) 应能提供开放的 API 形式供上层应用访问。

7.3 运营平台

7.3.1 基本要求

“转租转借监管难”和“租金收缴难”是租房管理过程中遇到的两大核心问题，系统智能分析、及时预警、强力管控，杜绝转租转借、房屋长期空置、恶意欠租行为，推进公共资源公平善用，提高监管决策能力。

7.3.2 主要功能及技术要求

运营平台的主要功能应符合下列要求：
a) 支持人员身份核验及信息登记，通过 1:1 比对身份证内照片与采集的人脸照片，核验人员身份，在布控范围内出现关注人员，系统立刻报警，输出告警现场图像、现场人脸图像，并将报警信息上传至平台（和/或上级平台）；
b) 支持录入租客身份信息，以及房源信息，包括楼幢、单元、房间信息；
c) 支持对合同管理、租金管理、维修派工等功能；
d) 支持对智能设备的设备资源、人员权限与配置的统一管理；
e) 支持保洁、带看等员工行为记录，通过相机等设备实现视频画面的采集和存储。

8 应用层技术要求

8.1 应用层概述

长租公寓（含公租房）智能化应用管理系统应实现实名认证、远程授权、移动执法、运营管理、客户端应用等功能，提供基于密码的安全应用，并应支持第三方安全云与业务云、第三方设备或系统的安全接入。

8.2 实名认证

管理系统应实现实名认证功能，采用人脸、指纹等生物特征识别技术、身份证、手机SIM卡等具有唯一身份标识并经实名认证的介质凭证，进行租住人员的身份识别与授权管理。

8.3 远程授权

管理系统后台应远程控制用户对智能设备的操作使用权限。

8.4 移动执法

长租公寓管理部门执法人员可通过手机APP/微信小程序等客户端程序进行移动管理，如进行实时数据查询、权限管理等操作。当发生违规或异常情况时，房屋管理部门可在线做出及时响应。

8.5 客户端应用

长租公寓承租人可通过手机APP/微信小程序等客户端程序实时提交设备故障报修、在线查看处理进度、提交问题反馈与建议等。

8.6 运营管理

长租公寓（含公租房）的运营管理包括房源信息管理、承租人信息管理、房间访问权限管理、设备状态管理、使用异常预警和非法闯入报警，并应符合下列要求：

a) 房源信息管理：应通过管理平台统一维护和管理房源相关信息，可实时查询长租房当前资源占用情况；
b) 承租人信息管理：应通过管理平台统一管理和维护承租人相关信息；
c) 房间访问权限管理：应通过远程授权功能控制房间门锁的操作权限，远程管理门锁的使用。在特定情况下（如发生欠费或违规行为），系统后台应可远程冻结用户的开门权限，开门权限被冻结后，用户暂时不能打开房门。一旦导致开门权限被冻结的条件被解除（如承租人缴清欠费或违规事项处理完毕），系统后台应立即远程解除门锁冻结状态，恢复门锁正常开关功能；
d) 设备状态管理：可实时显示门锁等联网设备的当前运行状态，可实时发现设备故障和进行排查处理；
e) 使用异常预警：结合门禁/门锁状态监控数据、人员出入数据、设备操作数据、承租合同和缴费信息等相关信息进行综合数据分析，当发现用户日常使用行为异常时，管理平台应做出预警，以便长租房管理方能够及时发现房源空置、转租转借、合同逾期等状况；
f) 非法闯入报警：当非授权用户尝试闯入时，系统应自动报警。根据实际情况需要，报警信息可与公安系统联动。

8.7 外部业务安全接入

外部业务实现安全接入应符合下列要求：

a) 长租房系统应采用开放式的“云+云”业务接入方式，支持与独立的第三方安全云、以及公安、人社、政企等部门的业务云进行对接，实现长租房管理运维、便民服务、增值业务等智能化新业务的快速接入；
b) 长租房系统在与外部安全云或业务云进行对接时，应采用标准和安全的业务SDK接口。

8.8 智能化物联网设备安全接入

智能化物联网设备实现安全接入应符合下列要求：

a) 长租房系统应采用开放式的“云+端”设备接入方式，支持第三方运营的智能化物联网设备或系统的安全接入，并可对其进行设备安全管理；
b) 应向第三方设备或系统提供长租房系统颁发的身份证书，作为其接入长租房系统时的安全信任根，并基于安全信任根建立安全通道和进行数据安全传输；
c) 长租房系统在与第三方设备或系统进行连接时，应采用标准和安全的设备 SDK 接口。

9 安全要求

9.1 基础设施安全要求

基础设施信息安全要求应符合GB/T 28847.3 5.2.2.1的要求。

9.2 平台安全要求

9.2.1 基本要求

用户及敏感数据在传输及存储时，应采用加密方式实现，其安全机制应包含数据安全、信息安全、管理安全和个人隐私保护安全。并应符合下列要求：

a) 通过在数据存储、数据传输及访问权限控制，实现全链路的安全防护；
b) 通过收集管理平台日志及设备告警日志，实时或定时上报给数据分析平台，进行攻击趋势分析，并接收告警事件，及时处理相应的威胁；
c) 数据安全应符合 GB/T 30146 的要求；
d) 信息安全应符合 GB 17859 的要求；
e) 管理安全应符合 GB/T 22080 或者 ISO/IEC 27001 的要求；
f) 个人隐私安全应满足 ISO/IEC 27018 的要求。

9.2.2 主要技术要求

平台层安全应符合下列技术要求：

a) 对于重要数据存储使用数据密钥进行 AES 加密后保存，数据密钥使用主密钥加密保护存储，由 KMS 密钥管理系统对主密钥存储管理，保护密钥的机密性，完整性和可用性，密文数据与数据密钥、主密钥管理分离存储；
b) 对传输通道使用 TLS/HTTPS 方式加密传输通道保护传输安全，对敏感数据应进行应用层加密，使用一机一密钥机制，防止单个密钥泄露影响批量数据安全。其中密钥的下发需要使用可信安全通道，通过工厂生产方式下发，保护根密钥安全；
c) 对数据管理上面，采用职权分离设计，程序管理权与数据管理权做分离。权限分配遵循最小权限原则，防止权限过渡分配。账号管理使用统一账号体系，减少账号分散式管理安全威胁，降低管理成本；
d) 建设物联网系统安全态势感知平台，针对上传的各类日志事件进行收集，建立针对平台及物联网设备攻击的深度学习模型，通过海量数据的输入不断训练模型，使得攻击的智能识别逐渐趋向精准。通过对上报事件进行聚合分析，使用已有的安全规则，对攻击事件影响范围、攻击方式进行快速分析处理；
e) 对于出现规模性告警事件的区域，应对安全运营人员做出相应风险预警提示，防止相应攻击扩大造成损失。

9.3 客户端安全要求

客户端应设计安全的身份鉴别方案，保证用户身份鉴别安全，具体要求如下：

a) 用户在首次注册及修改口令时，应有对用户的鉴别信息进行复杂度检查设计；
b) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证认证系统安全；
c) 客户端在设计时，对于敏感操作应对身份鉴别采用二次验证的方案。敏感操作如密码增加删除修改、指纹增加删除、解绑设备等；
d) 个人信息安全应满足 GB/T 35273 的要求。

9.4 应用层安全要求

应用层密码安全应符合下列要求：

a) 平台端可通过集成安全云服务或采用独立的安全云服务方式，为联网设备提供安全的云端密钥分发、密钥管理、身份鉴别、访问授权等密码管理与安全应用服务；
b) 平台和设备端应支持会话密钥协商，并支持基于安全硬件的密钥存储；
c) 长租房系统在进行密钥、人脸、指纹、密码、身份标识等敏感信息的加密传输与存储时，以及在进行设备认证和用户身份鉴别等密码运算时，应采用 SM4、SM2、SM3 等国家密码管理部门认可的密码算法；
d) 终端设备应一机一密，设备密钥的生成和存储应在安全模块（SE）内或安全的存储及执行环境里进行。设备密钥以 SE 唯一标识和设备唯一标识作为密钥分散因子，通过随机数分散后生成；对于无 SE 安全单元的低安全等级设备，其设备密钥可采用 DEV_ID 作为密钥分散因子，通过随机数分散后生成；
e) 联网设备和平台之间的敏感数据传输应使用通信密钥或基于通信密钥生成的会话密钥进行加密。通信密钥以设备密钥和时间戳作为密钥分散因子，通过随机数分散后生成；对于无 SE 的低安全等级设备，其通信密钥可采用设备唯一标识和时间戳作为密钥分散因子，通过随机数分散后生成。时间戳应定期更新。

9.5 安全模块（SE）要求

9.5.1 一般规定

模块以及其实现算法应具有型号或版本信息。每个模块应具有唯一识别信息，算法及实现代码应具有固定版本信息。

9.5.2 异常处理

模块应能捕获常见的软硬件异常，并在异常发生时不泄露敏感信息。

9.5.3 随机数

模块的随机数产生器必须经过评估，确保其产生的随机数具有足够的随机性。

9.5.4 访问权限控制

模块应具有代码和数据访问权限控制功能，保证外部调用者无法直接操作敏感数据。

9.5.5 环境适应性

改变模块的环境条件或操作条件不会影响其安全性（例如操作电压、时钟频率或环境温度超出模块工作范围）。

9.5.6 密码算法验证

模块应硬件支持常见商用密码算法，包括但不限于TDES、AES、RSA、SM2、SM4 等，并使用满足商用密码算法要求密钥长度。

9.5.7 密钥生成安全

模块产生的非对称密钥，应满足素数的素性检查，密钥长度要求等，模块不应支持私钥的导出功能。

密钥生产基于真随机数，保证密钥的随机性，解决弱密钥隐患。

9.5.8 密钥存储安全

模块内部存储器具备加密存储功能，保证密钥存储安全。

9.5.9 密钥使用安全

模块产生的密钥相关操作在芯片内部完成，密钥不出芯片，杜绝密钥泄露。

9.5.10 密钥使用安全

模块具备安全OS平台及硬件MPU确保全密钥使用权限安全可控

9.5.11 抗攻击能力要求

模块具有一定的防御侵入式、半侵入式攻击能力，保护敏感信息不被物理攻击设备获取和篡改。模块可以对抗电压攻击、频率攻击和温度攻击。当遇到电压攻击、频率攻击、温度攻击产生报警，自动销毁敏感数据或告知模块产生报警信号。