ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 智能门锁网络安全技术规范

Information security technology—Cybersecurity technical specification for smart lock products

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

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。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：公安部第三研究所、中国信息安全研究院有限公司、中移（杭州）信息技术有限公司、中国网络安全审查技术与认证中心、国家计算机网络与信息安全管理中心、浙江大华技术股份有限公司、杭州萤石软件有限公司、中山市锁业协会、云丁网络技术(北京)有限公司、北京奇虎科技有限公司、上海斗象信息技术有限公司、宁波市镇海神舟锁业有限公司、阿里巴巴（北京）软件服务有限公司、青岛海尔智能家电科技有限公司、上海嘉韦思信息科技有限公司、北京小米移动软件有限公司、移康智能科技（上海）股份有限公司、南京东屋电气有限公司、上海市质量监督检验技术研究院、工业和信息化部电子第五研究所、中国科学院信息工程研究所、中国信息通信研究院、华为技术有限公司、翼盾（上海）智能科技有限公司、浙江智贝信息科技有限公司、上海物盾信息科技有限公司、启明星辰信息技术集团股份有限公司、深圳市凯迪仕智能科技股份有限公司。

本文件主要起草人：刘继顺、陆臻、顾健、沈亮、张艳、孙永清、李海鹏、胡津铭、张智强、杨晨、路晓明、于晓杰、常涛、张屹、何清林、冯秀英、何曙、李乐言、潘月霖、舒首衡、李国柱、姚俊宁、朱易翔、周正达、徐梦宇、陈灿峰、朱鹏程、闵浩、李凤华、张昊星、赖东亮、苏祺云、吴其良、杜南、牛国君。

信息安全技术 智能门锁网络安全技术规范

1 范围

本文件规定了联网智能门锁系统中的智能门锁终端、接入网关、管理平台、控制端应用APP各组成部分以及通信连接网络的安全技术要求，给出了测试方法及安全等级划分。

本文件适用于智能门锁系统的网络安全设计、实现和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 15843—2017 信息技术 安全技术 实体鉴别

GB 21556—2008 锁具安全通用技术条件

GB/T 25069 信息安全技术 术语

GB/T 33474—2016 物联网 参考体系结构

GB/T 33745—2017 物联网 术语

GB/T 34975—2017 信息安全技术 移动智能终端应用安全技术要求和测试评价方法

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 36950—2018 信息安全技术 智能卡安全技术要求

GB/T 36951—2018 信息安全技术 物联网感知终端应用安全技术要求

GB/T 37024—2018 信息安全技术 物联网感知层网关安全技术要求

GB/T 37044—2018 信息安全技术 物联网安全参考模型及通用要求

GB/T 37076—2018 信息安全技术 指纹识别系统技术要求

GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求

3 术语和定义

GB 21556—2008、GB/T 25069、GB/T 33474—2016、GB/T 33745—2017、GB/T 34975—2017、GB/T 35273—2020、GB/T 36951—2018、GB/T 37024—2018、GB/T 37044—2018界定的以及下列术语和定义适用于本文件。

3.1

智能门锁 smart lock

以生物特征、电子标签、无线遥控编码、电子口令或远程控制指令等作为鉴别信息，由门锁终端、接入网关、管理平台以及控制端应用APP等部分组成的门锁信息系统。

3.2

相互鉴别 mutual authentication

实体双方均向对方提供身份保证信息的实体鉴别机制。

[来源：GB/T 15843.1—2017，3.18]。

3.3

CPU卡 CPU card

含有中央处理器（CPU）的IC卡。

3.4

关键安全信息 critical security information

与安全相关的信息，其被泄露或被修改后会危及智能门锁安全性。

注：例如用户登录鉴别信息、管理平台管理员鉴别信息、智能门锁终端鉴别信息等。

3.5

虚位口令 virtual password

在正确的口令前面和后面加上任意位数的字符的口令。

3.6

呈现攻击 presenting attacks

以干扰生物特征识别系统的操作为目的，针对生物特征数据采集模块的一种攻击行为。

4 缩略语

以下缩略语适用于本文件。

AP：无线接入点（Access Point）

APP：应用软件（Application Software）

CPU：中央处理器（Central Processing Unit）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

IC：集成电路（Integrated Circuit）

ID：标识（Identification）

IP：互联网协议（Internet Protocol）

KRACK：口令重置攻击（Key Reinstallation Attacks）

MAC：媒体访问控制（Media Access Control）

MCU：微控制单元（Microcontroller Unit）

NFC：近场通信（Near Field Communication）

PCB：印刷电路板（Printed Circuit Boards）

PIN：个人识别码（Personal Identification Number）

SSID：服务集标识（Service Set Identifier）

SSL：安全套接层（Secure Sockets Layer）

TCP：传输控制协议（Transmission Control Protocol）

UID：用户身份标识（User Identification）

WPA：Wi-Fi 保护访问（Wi-Fi Protected Access）

WPA2：Wi-Fi 保护访问 2（Wi-Fi Protected Access Two）

2D：二维（Two Dimensional）

3D：三维（Three Dimensional）

5 概述

5.1 智能门锁组成

智能门锁是一种物联网应用系统，用以实现门锁的用户识别、远程控制以及系统管理，主要包括智能门锁终端、接入网关、管理平台和控制端应用 APP 等组件，其整体组成形态如图 1 所示。

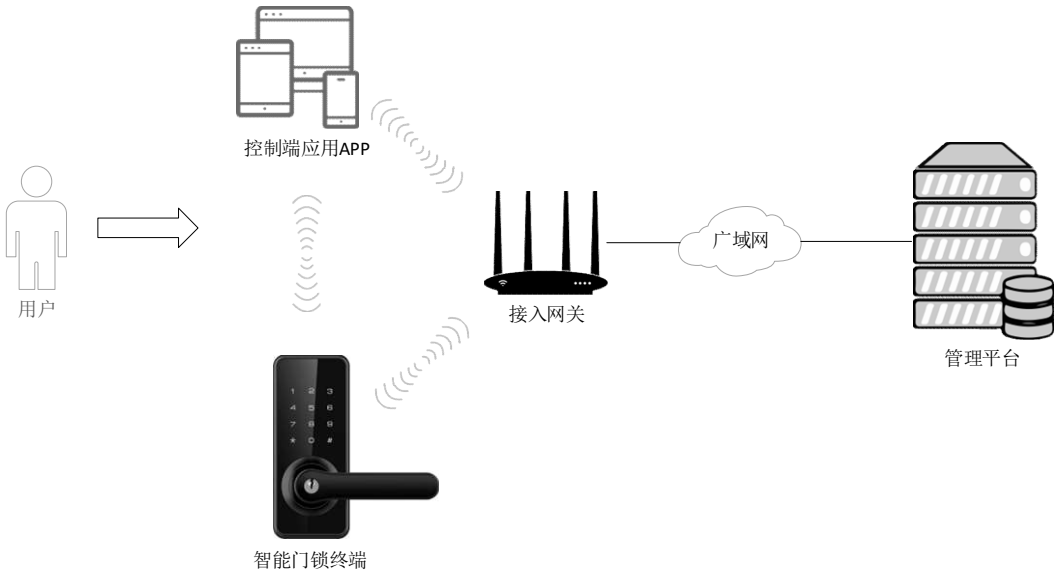

图 1 智能门锁系统组成

图1中:

a） 智能门锁终端是智能数据采集、接受远程控制，提供门锁启闭功能的智能软硬件实体。

b） 接入网关为智能门锁终端提供网络连接，提供协议转换、本地场景化服务和设备管理功能。

c） 智能门锁管理平台是后端智能门锁服务应用承载的功能实体，通过与智能门锁终端、智能门锁移动应用协同，实现智能门锁的具体应用服务。智能门锁管理平台具备智能门锁终端管理、智能感知信息融合处理、远程人机交互、远程控制等功能。

d） 控制端应用 APP 为实际使用智能门锁的终端用户提供远程控制、人机交互等功能。

e） 智能门锁系统的通信网络为智能门锁系统提供数据通信连接能力，实现智能数据采集、数据传输、数据处理等功能。智能门锁终端通过智能门锁接入网关或运营商网络与智能门锁管理平台、用户控制端连接，实现智能采集数据与控制指令的交互。

5.2 安全风险分析和安全分级

根据智能门锁系统的网络组成架构，本文件对智能门锁系统面临的安全风险进行了抽象，主要包括针对智能门锁终端、接入网关的硬件攻击风险，针对管理平台、控制端应用的软件攻击风险，以及针对近距离无线传输和远距离核心网络传输的攻击风险，具体分析见 A.1 和 A.2。

根据应用场景对网络安全防护能力的不同要求，将智能门锁系统的安全级别划分为两个等级：基本级、增强级，增强级网络安全防护能力高于基本级，**增强级在基本级基础上增加或者增强的技术要求用加粗字体表示。**

6 智能门锁网络安全技术要求

6.1 智能门锁终端安全技术要求

6.1.1 鉴别数据安全

6.1.1.1 口令鉴别安全

智能门锁使用口令作为鉴别信息时应满足：

a) 键盘有震动或声音反馈时，所有按键引起的震动或声音保持无差异或者随机反馈；
b) 在键盘无遮挡的设备上，支持虚位口令；
c) 支持多重身份鉴别。

6.1.1.2 生物信息鉴别安全

智能门锁使用生物信息鉴别用户身份时，生物识别模块应具备生物信息仿冒防范能力，满足：

a) 指纹识别模块具备防复制指纹仿冒、防指纹照片仿冒的能力，符合GB/T 37076-2018中6.1.5.7要求；
b) 人脸识别模块具备防复制人脸仿冒、防人脸照片仿冒、防面具仿冒的能力，符合GB/T 38671—2020中6.1.6.5要求；
c) 指纹识别模块具备检测假体或防止指纹假体仿冒行为；
d) 人脸识别模块具备防人脸视频仿冒、防人脸电脑图像合成仿冒、防假体面具仿冒能力，符合GB/T 38671—2020中6.2.6.6要求。
e) 具备其他类型生物识别模块具备防护呈现攻击的能力；
f) 具备生物识别模块具备发生上述攻击时暂停服务并发出告警的能力。

6.1.1.3 IC卡安全

智能门锁使用IC卡鉴别用户身份时，IC卡应满足：

a) 符合GB/T 36950-2018的要求；
b) 具备数据加密能力；
c) 具有防复制功能；
d) **IC卡采用CPU卡，其形态包括但不限于CPU智能卡、搭载安全载体且具备CPU卡功能的终端设备；**
e) **具备物理防御手段以防止侧信道攻击。**

6.1.2 固件安全

智能门锁终端固件应满足：

a) 在得到用户确认后，能进行固件更新机制；
b) 固件下载时，具备对更新文件来源进行校验的能力；
c) 具备防止中间人劫持或嗅探的安全下载通道；
d) 固件升级时，具备对更新文件完整性校验能力；
e) 固件升级失败，能够保持固件的可用性；
f) 具备防止未授权的固件回退的能力。

6.1.3 操作系统安全

智能门锁终端操作系统应满足：

a) 按照最小化原则，仅保留业务必需的应用模块、使用端口、控制权限；
b) 提供安全启动认证机制，禁止用户直接登录操作系统；

c) 具备操作系统更新机制和更新失效保护机制，更新前需要得到用户确认且告知更新结果。

6.1.4 应用安全

智能门锁终端应用应满足：

a) 在安装应用软件时，对软件安装包的完整性与来源的真实性进行校验；
b) 具备防范越权操控和身份仿冒的能力；
c) 安装满足业务安全功能需求的软件并正确配置及使用；
d) 按照策略进行补丁更新和升级，保证所更新的数据是来源的真实性和完整性；
e) 应用软件更新失败时，保持应用软件的可用性；
f) 具备防逆向、反编译能力。

6.1.5 接入认证

6.1.5.1 终端标识

针对智能门锁终端标识，应满足：

a) 具备可用于通信识别的唯一标识；
b) 设备标识具备防篡改机制。

6.1.5.2 网络接入认证

针对网络接入认证，应满足：

a) 在接入网络时，智能门锁终端应采用遵循 GB/T 15843-2017 的预共享密钥鉴别机制向接入网络证明其网络身份；
b) 智能门锁终端与管理平台、接入网关、控制端采用相互鉴别机制，鉴别机制采用 GB/T 15843-2017 的基于数字证书的接入机制。

6.1.5.3 账户与口令

智能门锁终端账户与口令安全要求应满足：

a) 添加用户、删除用户、恢复出厂设置等重要操作仅能由授权管理员进行操作，且操作前验证管理员身份；
b) 具备防止穷举口令攻击的能力，针对虚位口令的防穷举攻击机制能根据实际输入的口令长度增加限制；
c) 智能门锁终端不应采用默认口令，恢复出厂设置后，要求用户立即设置新口令，口令有复杂度要求。

6.1.6 访问控制

智能门锁终端的访问控制功能应满足：

a) 遵循最小权限原则对用户、控制端、管理平台分配智能门锁操作权限；
b) 能设置网络访问控制策略，只允许授权的网络通信单元通过网络访问和操作智能门锁。

6.1.7 通信安全

6.1.7.1 通信端口控制

针对通信端口控制，应满足：

a) 遵循最小配置原则，禁用非必要的通信端口；

b) 支持在线动态启用或者禁用特定的通信端口，启用或者禁用特定通信端口时应仅允许由授权用户操作。

6.1.7.2 传输可靠性

智能门锁终端应具备保障传输可靠性的机制，满足：

a) 具备通信完整性校验机制，进行数据传输的完整性保护；

b) 发生通信延时或中断时具备通信恢复机制；

c) 具备冗余链路，保证传输链路可靠性。

6.1.7.3 传输保密性

智能门锁终端通过有线通信或者无线通信方式与其他组件通信时，应满足：

a) 与接入网关之间的数据传输采用保密措施；

b) 与管理平台之间的数据传输采用保密措施；

c) 与控制端应用APP之间的数据传输采用保密措施；

d) 与智能钥匙之间的数据传输采用保密措施。

6.1.8 数据安全

6.1.8.1 数据采集安全

智能门锁终端采集数据时，应满足：

a) 数据采集前，明确告知用户采集数据范围、采集目的和采集方式等信息；

b) 数据采集时，满足最少够用原则，不应过度采集。

6.1.8.2 数据存储安全

智能门锁终端存储数据时，应满足：

a) 具备数据机密性保护机制，对重要数据进行加密处理；

b) 具备数据完整性保护机制，实现对鉴别数据、审计数据的完整性保护。

6.1.8.3 数据销毁安全

智能门锁终端应具备数据销毁机制，对废弃数据及时安全销毁。

6.1.9 个人信息安全

智能门锁终端的收集、存储个人信息时，应符合 GB/T 35273—2020 中第 5 章和第 6 章的安全要求。

6.1.10 安全审计

智能门锁终端设备应具备对安全事件的审计记录功能，满足：

a) 审计范围覆盖用户在智能门锁终端中的关键操作、重要行为、业务资源使用情况等重要事件；

   1) 对鉴别机制的任何使用，包括智能门锁终端与应用服务平台相互验证成功与失败等；

   2) 通信会话的中止，包括设备的正常中止和非正常中止；

3) 对智能门锁终端的关键操作。

b) 事件记录包含事件的日期和时间、事件类型、主体标识、客体标识和结果；

c) 本地审计记录具备存储容量保护措施，防止存储空间超过阈值后审计记录被破坏；

d) 保证审计记录向管理平台的传输安全。

6.1.11 入侵防范

应能限制其他设备与智能门锁终端通信的地址，避免智能门锁终端对陌生地址的攻击行为，发生连续鉴别失败、外力强拆等安全事件时，应能发出告警。

6.1.12 其他

6.1.12.1 接口安全

智能门锁硬件接口应满足：

a) 调试功能接口在出厂时设置为默认关闭；

b) 烧录/调试功能接口，如JTAG、串口等，具备鉴别用户身份和访问权限能力，禁止直接登录；

c) 不应保留烧录/调试功能接口。

6.1.12.2 异常情况响应

电源电量不足引起的智能门锁开启控制异常时，应具备应急充电接口，能够应急充电。

6.2 接入网关安全技术要求

6.2.1 接入认证

6.2.1.1 网关标识

对于智能门锁接入网关的标识，应符合 6.1.5.1 终端标识中 a)-b)的要求。

6.2.1.2 网络接入认证

a) 接入网关应能对接入的智能门锁终端进行设备身份鉴别；

b) **接入网关与智能门锁终端、管理平台、控制端进行相互鉴别机制，采用遵循GB/T 15843-2017的预共享密钥鉴别机制或采用遵循GB/T 15843-2017的基于数字证书的接入鉴别机制。**

6.2.1.3 认证失败处理

接入网关应具备接入认证失败的处理能力，满足：

a) 当认证应答超过规定时限时，接入网关系统能终止与待接入终端之间的当前通信会话；

b) 在经过一定次数的认证失败后，接入网关系统能终止由接入终端发起的建立会话的尝试，在一定的时间间隔后才允许继续接入；

c) 在经过一定次数的认证失败后，采集和记录当前尝试鉴别者的信息（指纹、人脸信息等），并上报给用户或者管理员。

6.2.2 访问控制

接入网关应能控制智能门锁终端和管理平台的网络访问，满足：

a) 能制定访问控制策略，防止资源被非法访问和非法使用，访问控制策略包含用户或者设备身份和基于IP地址及端口、用户/用户组、读/写等操作、有效时间周期等的两种及以上构成的组合；
b) 能控制相同网络内部的相互访问；
c) 能控制不同网络区域之间的访问；
d) 能支持接入终端白名单机制，限制对接入网关的通信访问。

6.2.3 通信安全

6.2.3.1 传输可靠性

对于智能门锁接入网关的传输可靠性，应满足：

a) 对于智能门锁接入网关的传输可靠性，符合6.1.7.2传输可靠性中a)-b)的要求。
b) 采用安全通信机制，防止重放攻击和中间人攻击。

6.2.3.2 传输保密性

对于智能门锁接入网关的传输保密性，应符合6.1.7.3传输保密性中a)-c)的要求。

6.2.4 数据安全

6.2.4.1 数据存储安全

接入网关在数据存储安全方面，应满足：

a) 对存储在接入网关中的数据进行保护，避免非授权的访问，重要数据包括但不限于终端设备或用户的鉴别信息、网关配置信息、安全策略、审计信息等；
b) 对于接入网关在数据存储安全方面，符合6.1.8.2数据存储安全中b)的要求。

6.2.4.2 数据销毁安全

智能门锁接入网关应具备数据销毁机制，废弃数据应及时安全销毁。

6.2.5 个人信息安全

智能门锁接入网关的存储个人信息时，应符合 GB/T 35273—2020 中第 5 章和第 6 章的安全要求。

6.2.6 安全审计

针对接入网关安全审计，应满足：

a) 符合6.1.10安全审计的要求；
b) 记录恶意攻击、异常行为、病毒/木马程序等的入侵行为。

6.2.7 入侵防范

a) 针对接入网关入侵防范，应满足：接入网关具备对接入终端的接入防护能力，支持应用指定的通信协议和数据内容格式检查的数据包过滤，并丢弃不符合过滤要求的数据包；
b) 仅开放应用相关的通信端口；
c) 能针对网关的恶意攻击、异常行为、病毒/木马程序等的入侵行为进行检测和防护；

d) 拒绝和丢弃不可鉴别的通信网通信数据，且记录相应的日志。

6.2.8 其他

6.2.8.1 失效保护

接入网关应具备失效保护能力，保证设备异常时安全策略的正确性和可用性。

6.3 管理平台安全技术要求

6.3.1 接入认证

智能门锁管理平台的身份鉴别应满足：

a) 采用鉴别技术对用户登录、设备通信进行身份鉴别；
b) 提供并启用登录失败处理功能；
c) 提供并启用用户身份标识唯一检查功能，保证不存在重复用户身份标识，提供并启用用户鉴别信息复杂度检查功能；
d) 不应明文存储鉴别信息；
e) 采用两种或两种以上组合的鉴别技术来进行身份鉴别；
f) 进行系统安全相关的关键操作前进行用户二次身份鉴别。

6.3.2 访问控制

智能门锁管理平台的访问控制应满足：

a) 控制用户的访问权限，按安全策略要求控制用户对管理平台的访问；
b) 控制管理平台上应用与应用之间相互调用的权限,按照安全策略要求控制应用对其他应用里的用户数据或特权指令等资源的调用。

6.3.3 通信安全

6.3.3.1 传输可靠性

对于智能门锁管理平台的传输可靠性，应符合6.2.3.1传输可靠性要求。

6.3.3.2 传输保密性

对于智能门锁管理平台的传输保密性，应符合6.1.7.3传输保密性中a)-c)的要求。

6.3.4 应用安全

智能门锁管理平台的应用要求包括：

a) 管理平台的接入应用，应满足：
   1) 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；
   2) 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；
   3) 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。
b) 管理平台的接入设备，应满足：

1) 为每个智能门锁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) 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) 对接入平台的设备进行身份鉴别，只有经过鉴别，具有权限的设备才能接入业务平台进行后续应用操作；
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) 设备认证过程中如果使用随机数机制，应确保不可预测；
6) 对于支持应用账号绑定的设备，不应通过设备重置方式进行账号重新绑定，只有原账号解绑后才可进行重新绑定。

c) 管理平台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。

6.3.5 数据安全

6.3.5.1 数据采集安全

对于智能门锁管理平台的数据采集安全，应符合6.1.8.1数据采集安全要求。

6.3.5.2 数据访问控制

对智能门锁管理平台数据访问控制要求包括：

a) 应支持权限控制功能，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；
b) 涉及重要业务数据及其相关关键安全信息的文件应进行权限控制，只能由授权用户访问；
c) 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。

6.3.5.3 数据安全存储

智能门锁管理平台的数据安全存储功能应满足：

a) 支持分等级的数据加密方法，根据数据重要程度采用不同的安全保密存储机制；
b) 支持密钥安全存储，例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；
c) 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及时发现。

6.3.5.4 数据销毁安全

智能门锁管理平台数据销毁功能应支持完全清除数据，清除数据后不可恢复，在销毁数据前应提前明确提示用户，并由用户确认是否销毁后执行。

6.3.5.5 数据备份与恢复

智能门锁管理平台的数据备份与恢复功能应满足：

a) 具备对各类数据和文件进行归档的能力，并定期对临时数据及文件自动清理，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；
b) 备份数据完整有效且保密存储；

c） 恢复数据时校验备份数据的完整性。

6.3.5.6 数据融合处理

智能门锁管理平台的数据融合处理功能应满足：

a） 能够对来自不同智能门锁终端和接入网关的数据进行数据融合处理，使不同种类的数据可在同一平台被使用；

b） 对不同数据之间的依赖关系和制约关系进行智能处理。

6.3.6 个人信息安全

智能门锁管理平台的收集、存储个人信息时，应符合 GB/T 35273—2020 中第 5 章和第 6 章的安全要求。

6.3.7 安全审计

智能门锁管理平台的安全审计功能应满足：

a） 审计范围应覆盖到用户在管理平台中的关键操作、重要行为、业务资源使用情况等重要事件，包括但不限于以下事件：

1） 审计功能的启动和关闭；
2） 导出、另存和删除审计日志；
3） 设置鉴别尝试次数；
4） 设置审计日志报警门限值；
5） 鉴别机制的使用；
6） 用户的创建、修改、删除和授权；
7） 通过控制端应用对智能门锁设备进行的操作；
8） 设备状态的变化；
9） 其他系统参数配置和管理安全功能行为的操作。

b） 对审计记录进行保护，避免非授权的访问、篡改、覆盖或删除等；

c） 根据业务功能需求提供与其相关的审计信息及审计分析报告；

d） 相关审计记录包括事件日期、时间、用户、类型、描述和结果等，审计记录留存时间超过6个月；

e） 具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；

f） 具备自动化审计功能，监控明显异常操作并响应；

g） 支持审计日志导出功能；

h） 对审计记录进行非明文存储；

i） 记录恶意攻击、异常行为、病毒/木马程序等的入侵行为。

6.3.8 其他

6.3.8.1 资源控制

智能门锁管理平台的资源控制功能应满足：

a） 限制对管理平台访问的最大并发会话连接数；

b） 提供资源控制不当的报警及响应；

c） 在会话处于非活跃状态一定时间后终止会话连接；

d） 对用户与管理平台通信过程中的重要数据加密，具备对访问、通信等行为的防抵赖功能。

6.3.8.2 抗数据重放

智能门锁管理平台的抗数据重放功能应满足：

a) 能鉴别数据的新鲜性，避免历史数据的重放攻击；
b) 能鉴别历史数据的非法修改，避免数据的修改重放攻击。

6.4 控制端应用 APP 安全技术要求

6.4.1 应用安全

6.4.1.1 安装要求

智能门锁控制端应用APP的安装步骤应满足：

a) 安装过程经用户明确许可；
b) 包含可有效表征供应者或开发者身份的签名信息、软件属性信息；
c) 在安装的过程中，可随时取消安装；
d) 正确安装到相关移动智能终端上，并生成相应的图标；
e) 下载和安装过程中，不得捆绑下载其他应用软件；
f) 在安装智能门锁控制端应用APP时，遵循最小安装原则，不应安装本软件功能说明文档中未加说明的额外功能，不安装用户未知和未允许的第三方应用；
g) 以用户可见的方式进行安装，有安装界面；
h) 安装时调用终端资源和终端数据向用户明示,并得到授权后使用该终端资源和数据；
i) 控制端应用在安装好后不应强制用户重启设备；
j) 未经用户允许不应获取已安装的第三方应用信息；
k) 不应对终端操作系统和其他应用软件的正常运行造成影响。

6.4.1.2 卸载要求

智能门锁控制端应用APP卸载后，不影响移动智能终端的正常使用，应满足：

a) 提供卸载软件的方式，用户能够随时卸载应用软件；
b) 卸载时将其安装进去的文件全部卸载，自动运行权限需要得到用户的明确授权；
c) 能够完全删除安装和使用过程中产生的资源文件、配置文件和用户数据，删除用户使用过程中生成的数据时应有提示；
d) 能够恢复修改的系统配置信息；
e) 能够彻底卸载应用软件,不应在系统中留下应用软件的临时文件和活动程序或模块；
f) 卸载后不影响终端操作系统和其他应用软件的功能。

6.4.1.3 更新机制

智能门锁控制端应用APP应支持软件的更新，满足：

a) 有更新版本时，提示用户更新，不应未经用户允许自动更新；
b) 具备保证软件更新的时效性和准确性的安全机制；
c) 更新失败应能回退到更新前的版本。

6.4.2 接入认证

6.4.2.1 身份鉴别

智能门锁控制端应用APP控制智能门锁开启或读取用户信息时，应满足：

a) 在用户访问应用业务前，智能门锁控制端应用APP对用户身份进行鉴别；
b) 具备登录超时后的锁定或注销功能；
c) 具备防暴力破解的鉴别失败处理措施。

6.4.2.2 口令安全机制

智能门锁控制端应用APP使用口令作为鉴别信息时，应满足：

a) 口令信息不应以明文形式显示和存储；
b) 不应默认保存用户上次的账号及口令信息；
c) 具备口令强度检查机制；
d) 具备口令时效性检查机制；
e) 修改或找回口令时，具备验证机制；
f) 在使用过程中具备防键盘劫持机制；
g) 具备口令鉴别失败处理能力；
h) 口令不应以明文传输。

6.4.3 访问控制

智能门锁控制端应用APP应满足：

a) 授权用户访问的内容不应超出授权范围；
b) 未得到用户许可前不应访问智能门锁终端的数据；
c) 未得到用户许可前不应对智能门锁终端数据进行修改和删除。

6.4.4 通信安全

6.4.4.1 传输可靠性

对于智能门锁控制端应用 APP 的传输可靠性，应符合 6.2.3.1 传输可靠性要求。

6.4.4.2 传输保密性

智能门锁控制端应用APP与智能门锁终端、接入网关、管理平台通信时，数据传输应采取保密措施。

6.4.5 数据安全

6.4.5.1 数据采集安全

对于智能门锁应用APP的数据采集安全，应符合6.1.8.1数据采集安全要求。

6.4.5.2 数据存储安全

智能门锁控制端应用 APP 应对关键安全信息数据进行安全加密存储。

6.4.5.3 数据销毁安全

智能门锁控制端应用 APP 应具备数据销毁机制，废弃数据应及时安全销毁。

6.4.6 个人信息安全

智能门锁控制端应用 APP 收集、存储、使用个人信息时应符合 GB/T 35273—2020 第 5

章、第 6 章和第 7 章的安全要求。

6.4.7 安全审计

智能门锁控制端应用 APP 发生网络交互时,APP 应记录日志，并传输到服务平台，应满足：

a) 对各项操作进行审计记录，可记录事件包括但不限于：
   1) 对鉴别机制的任何使用，包括控制端应用APP与管理平台、智能门锁终端相互验证成功与失败等；
   2) 通信会话的终止，包括控制端应用APP的正常中止和非正常中止；
   3) 对智能门锁终端的关键操作。
b) 事件记录包含事件的日期和时间、事件的类型、主题标识、客体标识和结果；
c) 本地审计记录具备存储容量保护措施，防止存储空间超过阈值后审计记录被破坏；
d) 保证审计记录向管理平台的传输安全。

7 智能门锁网络安全测试方法

7.1 智能门锁终端安全测试方法

7.1.1 鉴别数据安全

7.1.1.1 口令鉴别安全

智能门锁终端口令安全的测试方法和预期结果如下：

a) 检测方法：
   1) 观察智能门锁口令按键按下后的反馈是否一样；
   2) 观察按下智能门锁的口令按键后是否有对应的数字音频输出；
   3) 观察智能门锁是否支持虚位口令功能；
   4) 检查智能门锁是否具有多重鉴别功能。
b) 预期结果：
   1) 智能门锁的口令按键按下后的反馈是完全一样的或者反馈是足够随机的；
   2) 智能门锁的口令按键按下后音频模块不能识别 PIN 码，且无法输出对应的音频；
   3) 智能门锁支持虚位口令功能；
   4) 智能门锁支持除口令鉴别以外的多重鉴别。

7.1.1.2 生物信息鉴别安全

智能门锁使用生物信息鉴别用户身份时，测试方法和预期结果如下：

a) 检测方法：
   1) 检查指纹识别模块是否具备防复制指纹仿冒、防指纹照片仿冒的能力，是否符合 GB/T 37076-2018 中 6.1.5.7 要求；
   2) 检查人脸识别模块是否具备防复制人脸仿冒、防人脸照片仿冒、防面具仿冒的能力，是否符合 GB/T 38671—2020 中 6.1.6.5 要求；
   3) 检查指纹识别模块是否具备检测假体或防止指纹假体仿冒行为；
   4) 检查人脸识别模块是否具备防人脸视频仿冒、防人脸电脑图像合成仿冒、防假体面具仿冒能力，是否符合 GB/T 38671—2020 中 6.2.6.6 要求；

5) 检查其他类型生物识别模块是否具备防护呈现攻击的能力；
6) 发生上述攻击时观察生物识别模块是否暂停服务并发出告警。

b) 预期结果：
1) 指纹识别模块具备防复制指纹仿冒、防指纹照片仿冒的能力，符合 GB/T 37076-2018 中 6.1.5.7 要求；
2) 人脸识别模块是否具备防复制人脸仿冒、防人脸照片仿冒、防面具仿冒的能力，符合 GB/T 38671—2020 中 6.1.6.5 要求；
3) 指纹识别模块具备检测假体或防止指纹假体仿冒行为；
4) 人脸识别模块具备防人脸视频仿冒、防人脸电脑图像合成仿冒、防假体面具仿冒能力，符合 GB/T 38671—2020 中 6.2.6.6 要求；
5) 其他类型生物识别模块具备防护呈现攻击的能力；
6) 发生上述攻击时，生物识别模块暂停服务并发出告警。

7.1.1.3 IC 卡安全

智能门锁终端 IC 卡安全的测试方法和预期结果如下：

a) 检测方法：
1) 读取 IC 卡中的数据，观察数据中的口令是否不同；
2) 查看 IC 卡是否使用 CPU 卡；
3) 观察智能门锁程序中是否有对 IC 卡校验的代码；
4) 逆向智能门锁固件，提取出根密钥对比其他门锁的根密钥是否一样。

b) 预期结果：
1) IC 卡采用 CPU 卡；
2) 智能门锁对 IC 卡进行绑卡，认证时对 IC 卡的数据模块进行读写校验；
3) 智能门锁具有唯一的根密钥。

7.1.2 固件安全

智能门锁终端固件安全的测试方法和预期结果如下：

a) 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。

b) 预期结果：
1) 操作系统具有自动和手动更新功能；
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；
3) 固件下载链路可以确保可信，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，不能通过完整性校验，更新失败；
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。

7.1.3 操作系统安全

智能门锁终端操作系统安全的测试方法和预期结果如下：

a) 检测方法：
   1) 查看智能门锁终端操作系统的应用模块、使用端口、控制权限信息，满足最小化原则；
   2) 查看是否提供安全启动认证机制，默认账户常用空口令登录是否成功；
   3) 查看系统更新时是否获得最终用户授权，更新后是否通知更新结果。
b) 预期结果：
   1) 智能门锁终端操作系统的应用模板、使用端口、控制权限信息满足最小化原则；
   2) 智能门锁操作系统提供安全认证机制；
   3) 智能门锁操作系统更新时得到最终用户确认且告知更新结果。

7.1.4 应用安全

智能门锁终端应用安全的测试方法和预期结果如下：

a) 检测方法：
   1) 在安装应用软件时，是否对软件包的完整性与来源的真实进行校验；
   2) 查看智能门锁终端是否具备防范越权操作和身份仿冒的能力；
   3) 查看智能门锁终端安装软件是否满足业务安全功能需求，且是否正确配置及使用；
   4) 查看智能门锁终端是否具备软件更新升级功能，是否检查更新的数据来源，且判断软件来源的真实性和完整性；
   5) 查看软件更新失败时，是否保持应用软件的可用性；
   6) 查看智能门锁终端是否具备防逆向反编译能力。
b) 预期结果：
   1) 在安装应用软件时，智能门锁终端校验软件包的完整性和来源的真实性；
   2) 智能门锁终端具备防范越权操作和身份仿冒的能力；
   3) 智能门锁终端的安装软件满足业务安全功能需求，且发布软件配置正确；
   4) 智能门锁终端具备软件更新和升级功能，升级时校验更新数据的来源，并判断真实性和完整性；
   5) 智能门锁终端软件更新失败时，不影响应用软件的使用；
   6) 智能门锁终端具备防逆向反编译能力。

7.1.5 接入认证

7.1.5.1 终端标识

智能门锁终端标识的测试方法和预期结果如下：

a) 检测方法：
   1) 查看智能门锁终端是否有唯一标识，非授权用户是否可以更改；
   2) **查看智能门锁终端是否具备防篡改保护机制。**
b) 预期结果：

1) 智能门锁终端具备门锁的唯一标识，且非授权用户不能更改；
2) **智能门锁终端设备标识具备防篡改保护机制。**

7.1.5.2 网络接入认证

智能门锁终端网络接入认证的测试方法和预期结果如下：

a) 检测方法：
   1) 在智能门锁终端核查预共享密钥鉴别机制，抓取网络通信数据包进行分析；
   2) 核查智能门锁终端是否采用数字证书和数字签名，验证是否采用数字签名方式进行身份鉴别；
   3) 是否可以向接入网络证明其网络身份。
b) 预期结果：
   1) 在智能门锁终端核查预共享密钥鉴别机制；
   2) 智能门锁终端采用数字证书和数字签名方式进行身份鉴别；
   3) 可向接入网络证明其网络身份。

7.1.5.3 账号与口令

智能门锁终账号与口令的测试方法和预期结果如下：

a) 检测方法：
   1) 测试添加用户、删除用户、恢复出厂设置等重要操作是否需要验证管理员身份；
   2) 暴力破解智能门锁口令，观察智能门锁是否会自锁；
   3) 用默认口令尝试打开门锁。
b) 预期结果：
   1) 添加用户、删除用户、恢复出厂设置等重要操作需要验证管理员身份；
   2) 智能门锁具备防止穷举口令、指纹识别、人脸识别的功能；
   3) 用默认口令无法打开门锁。

7.1.6 访问控制

智能门锁终端访问控制的测试方法和预期结果如下：

a) 检测方法：
   1) 验证智能门锁终端是否可以对用户、控制端、管理平台配置合理的操作权限；
   2) 是否可以配置网络访问控制策略，配置的策略是否生效。
b) 预期结果：
   1) 智能门锁终端可以遵循最小权限原则对用户、控制端、管理平台配置合理的操作权限；
   2) 可配置网络访问控制策略，配置的策略生效。

7.1.7 通信安全

7.1.7.1 通信端口控制测试

智能门锁终端通信端口控制的测试方法和预期结果如下：

a) 检测方法：
   1) 扫描智能门锁是否开启业务需求以外的通信端口；
   2) 动态配置特定的通信端口。
b) 预期结果：

1） 智能门锁终端遵循最小配置原则，禁用非必要的通信端口；
2） 支持在线动态启用或者禁用特定的通信端口，启用或者禁用特定通信端口时应仅可由授权用户操作。

7.1.7.2 传输可靠性测试

智能门锁终端传输可靠性的测试方法和预期结果如下：

a) 检测方法：
   1） 拦截通信数据包，查看数据包中是否有校验传输数据完整性的校验数据；
   2） 检测智能门锁是否具有通信延时和中断的处理机制；
   3） 对通信过程进行重放攻击和中间人攻击。
b) 预期结果：
   1） 智能门锁具有通信完整性的校验机制；
   2） 智能门锁具有通信延时和中断机制；
   3） 智能门锁可以防止重放攻击和中间人攻击。

7.1.7.3 传输保密性测试

智能门锁终端传输可靠性的测试方法和预期结果如下：

a) 检测方法：
   1） 抓取与网关之间的数据传输数据包，查看数据包中是否采取保密措施；
   2） 抓取与平台之间的数据传输数据包，查看数据包中是否采取保密措施；
   3） 抓取与 APP 之间的数据传输数据包，查看数据包中是否采取保密措施；
   4） 抓取与遥控钥匙之间的数据传输数据包，查看数据包中是否采取保密措施。
b) 预期结果：
   1） 与网关之间的通信数据包采取了保密措施；
   2） 与平台之间的通信数据包采取了保密措施；
   3） 与 APP 之间的通信数据包采取了保密措施；
   4） 与遥控钥匙之间的通信数据包采取了保密措施。

7.1.8 数据安全

7.1.8.1 数据采集安全

智能门锁终端数据采集的测试方法和预期结果如下：

a) 检测方法：
   1） 数据采集前，查看用户手册、用户通知等信息中是否告知用户采集数据范围、采集目的和采集方式等信息；
   2） 数据采集时，查看数据内容是否与告知用户的数据内容一致。
b) 预期结果：
   1） 数据采集前，已通过用户手册、用户通知等途径告知用户采集数据范围、采集目的和采集方式等信息；
   2） 数据采集时，采集的数据与告知用户的数据内容一致。

7.1.8.2 数据存储安全

智能门锁终端数据存储的测试方法和预期结果如下：

a) 检测方法：

1） 查看智能门锁终端数据，对留存数据进行加密处理；
2） 查看智能门锁终端认证数据、审计数据完整性防护机制。

b) 预期结果：
1） 智能门锁终端重要数据进行加密处理，具备机密性防护机制；
2） 智能门锁终端数据具备完整性防护机制。

7.1.8.3 数据销毁安全

智能门锁终端数据销毁的测试方法和预期结果如下：

a) 检测方法：
查看智能门锁终端数据销毁时，是否有残留数据。

b) 预期结果：
智能门锁终端数据销毁时，数据及时安全销毁。

7.1.9 个人信息安全

智能门锁终端收集、存储个人信息安全的测试方法和预期结果如下：

a) 检测方法：
核查产品收集、存储个人信息时是否满足 GB/T 35273—2020 标准第 5 章、第 6 章中对应项的要求；

b) 预期结果：
产品符合 GB/T 35273—2020 标准中对应项的要求。

7.1.10 安全审计

智能门锁终端安全审计的测试方法和预期结果如下：

a) 检测方法：
1） 当用户对智能门锁终端设备进行操作时，检查对于关键操作、重要行为、业务资源使用情况是否进行日志记录，检查内容包括但不限于：
- 查看是否覆盖智能门锁终端与管理平台相互验证成功与失败信息；
- 查看是否记录通信会话中止信息；
- 查看是否记录对智能门锁终端关键操作的信息。

2） 查看事件记录是否包含事件的日期和时间、事件的类型、主体标识、客体标识和结果；
3） 查看本地审计记录是否有保护措施，以防止存储空间超过阈值后审计记录被破坏；
4） 查看审计记录向管理平台转移时是否采用安全传输方式。

b) 预期结果：
1） 当用户对设备进行操作时，设备会对用户的关键操作、重要行为、业务资源使用情况进行日志记录，记录内容包括但不限于：
- 覆盖智能门锁终端与管理平台相互验证成功与失败信息；
- 记录通信会话中止信息；
- 记录对智能门锁终端关键操作的信息。

2） 日志事件记录包含事件的日期和时间、事件的类型、主体标识、客体标识和结果；
3） 智能门锁终端对本地审计日志记录存在保护措施，防止存储空间超过阈值破坏审计记录；

4） 审计记录向管理平台转移时采用安全传输方式。

7.1.11 入侵防范

智能门锁终端入侵防范安全的测试方法和预期结果如下：

a) 检测方法：
查看是否具备限制其他设备与智能门锁终端通信的目标地址的能力。

b) 预期结果：
具备限制其他设备与智能门锁终端通信的目标地址。

7.1.12 其他

7.1.12.1 接口安全

智能门锁终端接口安全的测试方法和预期结果如下：

a) 检测方法：
1） 对于具备 JTAG、串口等烧录/调试的接口，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；
2） 查看调试功能的接口，是否在出厂时是否设置为默认关闭；
3） 检查是否保留烧录/调试功能接口。

b) 预期结果：
1） 对于具备 JTAG、串口等烧录/调试的接口，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，并禁止直接登录；
2） 具备调试功能接口出厂时设置默认关闭；
3） 未保留烧录/调试功能接口。

7.1.12.2 异常情况响应

智能门锁终端异常情况响应测试方法和预期结果如下：

a) 检测方法：
1） 查看智能门锁是否具备应急充电接口；
2） 触发电源电量不足引起智能门锁开启控制异常情况，查看应急充电是否生效。

b) 预期结果：
1） 智能门锁具备应急充电接口；
2） 触发电源电量不足引起智能门锁开启控制异常情况，能够应急充电。

7.2 接入网关测试方法

7.2.1 接入认证

7.2.1.1 网关终端标识

智能门锁接入网关标识的测试方法、预期结果参照 7.1.5.1

7.2.1.2 网络接入认证

智能门锁接入鉴别机制的测试方法和预期结果如下：

a) 检测方法：
1） 检查智能门锁接入网关是否提供多种鉴别方式，并与产品说明描述一致；

2) 检查多种鉴别方式是否可以有效使用；
3) 检查是否具备智能门锁终端设备标识在接入网关生命周期内具备唯一性；
4) 检查对鉴别机制是否可同时多种方式使用。

b) 预期结果：
1) 智能门锁接入网关具备鉴别机制；
2) 智能门锁接入网关的鉴别机制与产品说明描述一致；
3) 智能门锁终端设备标识在接入网关生命周期内具备唯一性；
4) 智能门锁接入网关支持同时多种方式使用。

7.2.1.3 认证失败处理

智能门锁接入网关鉴别失败处理的测试方法和预期结果如下：

a) 检测方法：
1) 检查智能门锁接入网关设备是否具备超时机制；
2) 设定会话超时重新鉴别的时间段，检查在设定的时间段内没有任何操作的情况下，接入网关是否锁定或者终止会话，用户再次激活会话是否需要重新鉴定；
3) 接设定会话鉴定失败最大阈值，重复尝试失败会话，检查接入网关是否具备阶段性锁定功能。

b) 预期结果：
1) 接入网关具备检查会话超时机制，会话超时后需重新鉴定；
2) 在设定会话超时重新鉴别的时间段没有任何操作的情况下，会话被锁定或终止会话，用户需要再次身份鉴别才能够重新管理和使用系统；
3) 尝试多次失败会话鉴别，接入网关会对用户 IP 地址等标识信息锁定；
4) 尝试多次失败会话鉴别，接入网关会对用户 IP 地址等标识信息锁定。

7.2.2 访问控制

智能门锁接入网关访问控制的测试方法和预期结果如下：

a) 检测方法：
1) 配置启动接入网关访问控制表，检查是否支持基于 IP 地址及端口、用户/用户组、读/写等操作、有效时间周期、重要性标记等的两种及以上构成的组合；
2) 在相同网络内部是否可以访问；
3) 在不同网络之间进行跨网访问；
4) 制定白名单，查看限定用户是否可以访问成功。

b) 预期结果：
1) 接入网关支持访问控制表等访问控制策略，支持基于 IP 地址及端口、用户/用户组、读/写等操作、有效时间周期、重要性标记等的两种及以上构成的组合；
2) 在相同网络内部，仅能控制范围内的访问可以访问成功；
3) 在不同网络，仅能控制范围内的访问可以访问成功；
4) 仅在白名单定义的用户可以接入网关进行访问。

7.2.3 通信安全

7.2.3.1 传输可靠性测试

传输可靠性的测试方法、预期结果参照 7.1.7.2。

7.2.3.2 传输保密性测试

传输保密性的测试方法、预期结果参照 7.1.7.3 的 1)-3)。

7.2.4 数据安全

7.2.4.1 数据存储安全

数据存储的测试方法、预期结果参照 7.1.8.2。

7.2.4.2 数据销毁安全

数据销毁的测试方法、预期结果参照 7.1.8.3。

7.2.5 个人信息安全

个人信息安全的测试方法、预期结果参照 7.1.9。

7.2.6 安全审计

安全审计的测试方法、预期结果参照 7.1.10。

7.2.7 入侵防范

智能门锁接入网关入侵防护的测试方法和预期结果如下：

a) 检测方法：
   1) 使用非规定类型通信协议与接入网关进行通信，检查接入网关是否进行转发；
   2) 使用非标准格式数据内容与接入网关进行通信，检查接入网关是否进行转发；
   3) 检查接入网关开放的通信端口与产品标准文档描述是否保持一致。
b) 预期结果：
   1) 接入网关仅转发指定的通信协议和数据内容格式，检查外部来源数据格式，丢弃不符合过滤要求的数据包；
   2) 接入网关开放设备端口与产品标准文档中描述保持一致。

7.2.8 其他

7.2.8.1 失效保护

智能门锁接入网关失效保护的测试方法和预期结果如下：

a) 检测方法：
   1) 对接入网关发起恶意攻击，查看是否进入保护状态；
   2) 接入网关恢复时，检查安全配置策略是否存在丢失。
b) 预期结果：
   1) 接入网关接受恶意攻击时，会自动开启自动保护状态；
   2) 接入网关恢复时，所有安全配置保持关闭前状态。

7.3 管理平台测试方法

7.3.1 接入认证

智能门锁管理平台身份鉴别的测试方法和预期结果如下：

a) 检测方法：
   1) 检查标识与鉴别策略与规程等相关文档，查看其是否有对用户进行鉴别的要

求；

2) 检查访问控制策略与规程等相关文档，查看其是否在所定义的时间段内，定义了连续登录失败的上限次数；检查系统配置文件，查看其是否满足定义的登录失败处理策略；

3) 检查标识与鉴别策略与规程等相关文档，查看其是否有对信息系统的用户进行唯一标识要求；

4) 查看系统设置是否能够强制执行最小口令复杂度，并且满足定义的口令复杂度规则；查看其在用户更新口令时，是否要求满足口令复杂度要求，新旧口令是否不同；查看是否对口令加密存储；查看其是否强制执行最小和最大生存时间限制，并满足定义的最小生存时间和最大生存时间；

5) 检查标识与鉴别策略与规程等相关文档，查看其是否有针对网络访问实施多因子鉴别的要求；检查网络访问机制，查看其是否实施多因子鉴别；

6) 检查标识与鉴别策略与规程等相关文档，查看其是否有防范暴力破解等攻击的能力要求，在不影响系统安全情况的前提下使用暴力破解方式测试系统是否能够对攻击进行防范。

b) 预期结果：

1) 标识与鉴别策略与规程等相关文档有对用户进行鉴别的要求；

2) 访问控制策略与规程等相关文档在所定义的时间段内，定义了连续登录失败的上限次数；系统配置文件满足定义的登录失败处理策略；

3) 标识与鉴别策略与规程等相关文档有对信息系统的用户进行唯一标识要求；

4) 系统设置能够强制执行最小口令复杂度，并且满足定义的口令复杂度规则；在用户更新口令时，要求满足口令复杂度要求，新旧口令不同；对口令进行加密存储；强制执行最小和最大生存时间限制，并满足定义的最小生存时间和最大生存时间；

5) 标识与鉴别策略与规程等相关文档有针对网络访问实施多因子鉴别的要求；网络访问机制实施多因子鉴别；

6) 标识与鉴别策略与规程等相关文档有防范暴力破解等攻击的能力要求，系统能够对暴力破解方式测试攻击进行防范。

7.3.2 访问控制

智能门锁管理平台访问控制的测试方法和预期结果如下：

a) 检测方法：

1) 检查访问控制策略与规程等相关文档，查看其是否有最小特权策略；检查最小特权策略，查看其为用户提供的访问权限是否满足其最小业务需求；

2) 检查访问控制策略与规程等相关文档，查看其是否有针对不同应用间互相调用的权限限制要求，查看应用之间针对用户数据或特权指令等资源的调用是否符合安全策略要求。

b) 预期结果：

1) 访问控制策略与规程等相关文档有最小特权策略；最小特权策略为用户提供的访问权限满足其最小业务需求；

2) 访问控制策略与规程等相关文档有针对不同应用间互相调用的权限限制要求，应用之间针对用户数据或特权指令等资源的调用符合安全策略要求。

7.3.3 通信安全

7.3.3.1 传输可靠性测试

传输可靠性测试的测试方法、预期结果参照 7.1.7.2。

7.3.3.2 传输保密性测试

传输保密性的测试方法、预期结果参照 7.1.7.3 的 1)-3)。

7.3.4 应用安全

智能门锁管理平台应用安全的检测方法和预期结果判定如下：

a) 检测方法：

1) 应用服务平台的应用接入认证，检测方法如下：

- 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；
- 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；
- 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；
- 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；
- 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。

2) 接入应用服务的设备，检测方法如下：

- 审查厂商提交的文档，查看是否为每个智能门锁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；
- 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；
- 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；
- 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。

3) 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。

b) 预期结果：

1) 应用服务平台的应用接入认证，结果判定如下：

- 构建应用标识体系，为每个应用分配唯一的身份标识；
- 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；
- 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；
- 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；
- 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。

2) 接入应用服务的设备，结果判定如下：
   - 能为每个智能门锁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；
   - 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；
   - 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；
   - 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；
3) 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，其中一种鉴别技术使用密码技术来实现。

7.3.5 数据安全

7.3.5.1 数据采集安全

数据采集的测试方法、预期结果参照 7.1.8.1。

7.3.5.2 数据访问控制

智能门锁管理平台数据访问控制的检测方法和预期结果如下：

a) 检测方法：
   1) 检查是否支持权限控制功能，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) 验证包含重要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。
b) 预期结果：
   1) 支持权限控制功能，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；
   2) 包含重要信息的文件有权限控制，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。

7.3.5.3 数据存储安全

智能门锁管理平台数据存储安全的检测方法和预期结果如下：

a) 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、账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。

b) 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；
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。
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；
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；
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；
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。

7.3.5.4 数据销毁安全

智能门锁管理平台数据销毁安全的检测方法和预期结果如下：

a) 检测方法：
查看管理平台是否具备数据销毁功能，若具备数据销毁机制，在操作数据销毁功能时是否明确提示用户，并由用户确认后执行。

b) 预期结果：
管理平台若具备数据销毁机制，在操作数据销毁功能前，明确提示用户，并得到用户确认后执行。

7.3.5.5 数据备份与恢复

智能门锁管理平台数据备份与恢复的检测方法和预期结果如下：

a) 检测方法：
1) 查看管理平台是否提供数据备份机制，备份数据是否保密存储；
2) 数据恢复时是否校验数据的可用性及完整性。

b) 预期结果：
1) 管理平台提供数据备份机制，备份数据进行保密存储；
2) 数据恢复时校验数据的可用性及完整性。

7.3.5.6 数据融合处理

智能门锁管理平台数据融合处理的检测方法和预期结果如下：

a) 检测方法：
1) 查看管理平台是否具备对多台智能门锁终端上传数据进行融合处理的能力；
2) **查看管理平台是否能对不同数据之间的依赖关系和制约关系进行智能处理。**

b) 预期结果：
1) 管理平台具备对多台智能门锁终端上传数据进行融合处理的能力；
2) **管理平台具备对不同数据之间的依赖关系和制约关系进行智能处理能力。**

7.3.6 个人信息安全

个人信息安全的测试方法、预期结果参照 7.1.9。

7.3.7 安全审计

智能门锁管理平台安全审计的测试方法和预期结果如下：

a) 检测方法：

1) 当用户对智能门锁管理平台设备进行操作时，检查对于关键操作、重要行为、业务资源使用情况是否进行日志记录，检查内容包括但不限于：
   - 审计功能的启动和关闭；
   - 导出、另存和删除审计日志；
   - 设置鉴别尝试次数；
   - 设置审计日志报警门限值；
   - 鉴别机制的使用；
   - 用户的创建、修改、删除和授权；
   - 通过控制端应用对智能门锁设备进行的操作；
   - 设备状态的变化。
2) 查看审计记录是否进行保护，避免非授权的访问、篡改、覆盖或删除等行为；
3) 查看管理平台是否提供审计信息及审计分析报告，以满足业务功能需求；
4) 产看审计报告存留时间是否满足超过 6 个月，审计记录是否包括事件日期、时间、用户、类型、描述和结果等信息；
5) **查看管理平台是否提供对审计记录数据的统计、查询、分析及报表生成的功能；**
6) **查看管理平台是否具备自动化审计功能，对于系统异常操作做出响应；**
7) **查看审计报告存留时间是否满足超过 12 个月；**
8) **查看审计报告日志是否支持转储和导出功能；**
9) **查看审计记录是否对重要数据进行加密处理；**
10) **查看管理平台是否具备汇聚服务范围内的审计数据，支持第三方审计；**
11) **查看是否记录恶意攻击、异常行为、病毒/木马程序等入侵行为。**

b) 预期结果：

1) 当用户对设备进行操作时，设备会对用户的关键操作、重要行为、业务资源使用情况进行日志记录，记录内容包括但不限于：
   - 审计功能的启动和关闭；
   - 导出、另存和删除审计日志；
   - 设置鉴别尝试次数；
   - 设置审计日志报警门限值；
   - 鉴别机制的使用；
   - 用户的创建、修改、删除和授权；
   - 通过控制端应用对智能门锁设备进行的操作；
   - 设备状态的变化。
2) 管理平台对审计记录进行保护，防止非授权的访问、篡改、覆盖或删除等行为；
3) 管理平台提供审计信息及审计分析报告功能；
4) 审计报告存留时间满足超过 6 个月，审计记录包括事件日期、时间、用户、类型、描述和结果等信息；

5) **管理平台提供对审计记录数据的统计、查询、分析及报表生成的功能；**
6) **管理平台具备自动化审计功能，对于系统异常操作做出响应；**
7) **审计报告存留时间满足超过 12 个月；**
8) **审计报告日志支持转储和导出功能；**
9) **审计记录对重要数据进行加密处理；**
10) **管理平台具备汇聚服务范围内的审计数据，支持第三方审计；**
11) **查看记录恶意攻击、异常行为、病毒/木马程序等入侵行为。**

7.3.8 其他

7.3.8.1 资源控制

智能门锁管理平台资源控制的测试方法和预期结果如下：

a) 检测方法：
   1) 检查访问控制策略与规程等相关文档，查看其是否定义了平台访问的最大并发会话连接数等资源配额；测试并发会话控制机制，验证其对所定义的账号的最大并发会话连接数是否满足要求；
   2) 检查访问控制策略与规程等相关文档，查看其是否定义了资源控制不当的报警及响应机制；
   3) 检查访问控制策略与规程等相关文档，查看其是否定义了实施会话锁定时未活动的最大时间段；检查会话管理配置文件，查看其是否按照要求进行了配置；测试会话锁定机制，验证在定义的时间之内会话未活动是否会被锁定，验证用户主动发起锁定指令时是否能够实施会话锁定；
   4) **检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否有符合国家密码管理法律法规的通信加密和签名验签算法及设施的要求；检查通信加密和签名验签设施已获取的证书、测评报告等相关材料，查看其是否满足国家密码管理法律法规；**
   5) **检查系统与通信保护策略与规程、系统设计说明书等相关文档，查看其是否定义了服务水平阈值，并对服务水平进行监测的要求；测试当服务水平降低到预先规定的阈值时系统是否进行告警。**

b) 预期结果：
   1) 访问控制策略与规程等相关文档定义了平台访问的最大并发会话连接数等资源配额；平台对所定义的账号的最大并发会话连接数满足要求；
   2) 访问控制策略与规程等相关文档定义了资源控制不当的报警及响应机制；
   3) 访问控制策略与规程等相关文档定义了实施会话锁定时未活动的最大时间段；会话管理配置文件按照要求进行了配置；在定义的时间之内会话未活动会被锁定，用户主动发起锁定指令时能够实施会话锁定；
   4) **系统与通信保护策略与规程、系统设计说明书等相关文档有符合国家密码管理法律法规的通信加密和签名验签算法及设施的要求；通信加密和签名验签设施已获取的证书、测评报告等相关材料满足国家密码管理法律法规；**
   5) **系统与通信保护策略与规程、系统设计说明书等相关文档定义了服务水平阈值，并对服务水平进行监测的要求；当服务水平降低到预先规定的阈值时系统能够进行告警。**

7.3.8.2 抗数据重放

智能门锁管理平台抗数据重放的测试方法和预期结果如下：

a) 检测方法：
   1) 重放历史认证鉴别数据，检查管理平台是否具备避免历史数据的重放攻击能力；
   2) 修改历史认证鉴别数据，检查管理平台是否具备避免数据的修改重放能力。
b) 预期结果：
   1) 管理平台具备避免历史数据的重放攻击能力；
   2) 管理平台具备避免数据的修改重放能力。

7.4 控制端应用 APP 测试方法

7.4.1 应用安全

7.4.1.1 安装要求

智能门锁控制端应用APP安装的测试方法和预期结果如下：

a) 检测方法：
   1) 在移动智能终端上指定位置安装智能门锁控制端应用 APP；
   2) 检查智能门锁控制端应用 APP 是否包含供应者或开发者的签名信息、软件属性信息（如名称、版本信息和描述等）；
   3) 检查是否未经用户允许获取已安装的第三方应用信息；
   4) 如果智能门锁控制端应用 APP 安装时调用终端资源和终端数据，核查是否向用户明示，并在得到授权后使用该终端资源和数据；
   5) 运行智能门锁控制端应用 APP，检查是否对终端操作系统、其他应用软件（包括预置应用软件）的使用造成影响。
b) 预期结果：
   1) 能够安装到移动智能终端上，并生成相应图标；
   2) 包含供应者或开发者的签名信息、软件属性信息；
   3) 未经用户允许未获取已安装的第三方应用信息；
   4) 安装时如果调用终端资源和终端数据向用户明示，并在得到授权后使用该终端资源和数据；
   5) 智能门锁控制端应用 APP 安装后，终端操作系统和其他应用软件仍能正常使用。

7.4.1.2 卸载测试

智能门锁控制端应用APP卸载的测试方法和预期结果如下：

a) 检测方法：
   1) 卸载智能门锁控制端应用 APP，检查其安装及使用生成的文件和数据是否能完全删除；
   2) 检查删除用户数据时（如业务数据）是否有提示；
   3) 检查是否对终端操作系统、其他应用软件（包括预置应用软件）的使用造成影响。
b) 预期结果：
   1) 卸载时能够将其安装及使用过程产生的数据全部删除；
   2) 删除用户数据时能够提示用户授权；

3) 卸载后复原系统配置信息(如注册表)等；
4) 卸载后系统软件和其他应用软件仍能正常使用。

7.4.1.3 更新机制测试

智能门锁控制端应用APP更新的测试方法和预期结果如下：

a) 检测方法：
   1) 检查智能门锁控制端应用 APP 是否提供软件的更新功能；
   2) 检查智能门锁控制端应用 APP 是否提供安全机制，从而保证更新的时效性（如自动升级、更新通知等）和准确性（如完整性校验）。
b) 预期结果：
   1) 具备升级功能；
   2) 更新过程中，采用安全机制保证升级的时效性和准确性。

7.4.2 接入认证

7.4.2.1 身份鉴别测试

智能门锁控制端应用APP身份鉴别的测试方法和预期结果如下：

a) 检测方法：
   1) 检查在用户访问应用业务前，智能门锁控制端应用 APP 是否对其身份进行鉴别；
   2) 连续尝试登录失败时，检查智能门锁控制端应用 APP 是否具备鉴别失败处理措施（如锁定账号等）；
   3) 用户登录后长时间不进行任何操作。
b) 预期结果：
   1) 只有身份认证成功的应用用户才能使用智能门锁控制端应用 APP；
   2) 具备鉴别失败处理措施；
   3) 具备登录超时后的锁定或注销功能。

7.4.2.2 口令安全机制测试

智能门锁控制端应用APP口令安全机制的测试方法和预期结果如下：

a) 检测方法：
   1) 在智能门锁控制端应用 APP 中输入口令，检查口令是否以明文形式显示或存储；
   2) 检查智能门锁控制端应用 APP 是否默认保存用户上次的账号及口令信息；
   3) 检查智能门锁控制端应用 APP 是否具备口令强度检查机制（如口令长度、复杂度要求等）；
   4) 检测智能门锁控制端应用 APP 是否具备口令时效性检查机制（如主动提示用户定期修改口令等）；
   5) 检测智能门锁控制端应用 APP 在修改或找回口令时，是否具备验证机制（如验证手机号码等）；
   6) 检查智能门锁控制端应用 APP 是否具备防键盘劫持机制；
   7) 检查口令是否以明文或不安全形式传输。
b) 预期结果：
   1) 口令在使用、存储过程中不出现明文；

2) 未保存用户上次的账号及口令信息；
3) 具备口令强度检查机制，初始化及修改用户口令时，能够根据策略检查输入口令的长度和复杂度，若输入的口令不符合口令强度要求，能够提示，并要求重新设置有效口令；
4) 具备口令时效性检查机制，能够主动提示用户修改口令；
5) 修改或找回口令时，具备验证机制，以防止口令的被非授权获取或篡改；
6) 口令在使用过程中具备防键盘劫持机制，无法劫持获取用户输入的口令；
7) 口令没有明文传输，且以安全形式加密传输。

7.4.3 访问控制

智能门锁控制端应用APP访问控制的测试方法和预期结果如下：

a) 测试方法：
   1) 用户成功登录后，分别访问其授权和非授权的业务；
   2) 检查终端应用软件访问终端数据前是否明确得到终端操作系统用户的许可。
b) 预期结果：
   1) 应用用户仅能访问授权业务；
   2) 未得到终端操作系统用户明确许可前，终端应用软件不应访问终端数据。

7.4.4 通信安全

7.4.4.1 传输可靠性测试

传输可靠性的测试方法、预期结果参照 7.1.7.2。

7.4.4.2 传输保密性测试

传输保密性的测试方法、预期结果参照 7.1.7.3 的 1)-3)。

7.4.5 数据安全

7.4.5.1 数据采集安全

数据采集的测试方法、预期结果参照 7.1.8.1。

7.4.5.2 数据存储安全

智能门锁控制端应用APP数据存储安全的测试方法与预期结果如下：

a) 测试方法：

处理用户个人数据（如金融账户、联系人信息、聊天信息等）时，检查应用软件是否以明文形式写入文件中。

b) 预期结果：

不以明文形式将用户个人数据写到任何文件中。

7.4.5.3 数据销毁安全

智能门锁控制端应用 APP 数据销毁安全的检测方法和预期结果如下：

a) 检测方法：

查看 APP 是否具备数据销毁功能，若具备数据销毁机制，在操作数据销毁功能时是否明确提示用户，并由用户确认后执行。

b) 预期结果：

APP 若具备数据销毁机制，在操作数据销毁功能前，明确提示用户，并得到用户确认后执行。

7.4.6 个人信息安全

个人信息安全的测试方法、预期结果参照 7.1.9。

7.4.7 安全审计

智能门锁控制端应用 APP 安全审计的测试方法和预期结果如下：

a) 检测方法：

1) 当用户对智能门锁管理平台设备进行操作时，检查对于关键操作、重要行为、业务资源使用情况是否进行日志记录，检查内容包括但不限于：
   - 对鉴别机制的任何使用（如控制端应用APP与管理平台、智能门锁终端相互验证成功与失败等）；
   - 通信会话的终止（包括控制端应用APP的正常中止和非正常中止）；
   - 对智能门智能门锁终端的关键操作。
2) 查看审计记录是否进行保护，避免非授权的访问、篡改、覆盖或删除等行为；
3) 查看管理平台是否提供审计信息及审计分析报告，以满足业务功能需求；
4) 查看审计报告存留时间是否满足超过 6 个月，审计记录是否包括事件日期、时间、用户、类型、描述和结果等信息；
5) 抓取包含审计记录的报文查看是否明文传输。

b) 预期结果：

1) 当用户对设备进行操作时，设备会对用户的关键操作、重要行为、业务资源使用情况进行日志记录，记录内容包括但不限于：
   - 对鉴别机制的任何使用（如控制端应用APP与管理平台、智能门锁终端相互验证成功与失败等）；
   - 通信会话的终止（包括控制端应用APP的正常中止和非正常中止）；
   - 对智能门锁终端的关键操作。
2) 管理平台对审计记录进行保护，防止非授权的访问、篡改、覆盖或删除等行为；
3) 管理平台提供审计信息及审计分析报告功能；
4) 审计报告存留时间满足超过 6 个月，审计记录包括事件日期、时间、用户、类型、描述和结果等信息；
5) 审计记录非明文传输。

附录 A

（资料性）

智能门锁安全风险分析

A.1 概述

根据智能门锁的组网体系架构，其安全风险划分为以下五个方面：智能门锁安全风险（针对智能门锁设备的攻击）、控制端应用安全风险（针对智能门锁控制端应用 APP 的攻击）、近场通信安全风险(针对 Wi-Fi、ZigBee、蓝牙、433 和 315 等通信方式的攻击)、网络安全风险（针对家庭智能网关和有线数据拦截的攻击）和应用安全风险（针对智能门锁云平台的攻击）。具体如图 A.1 所示：

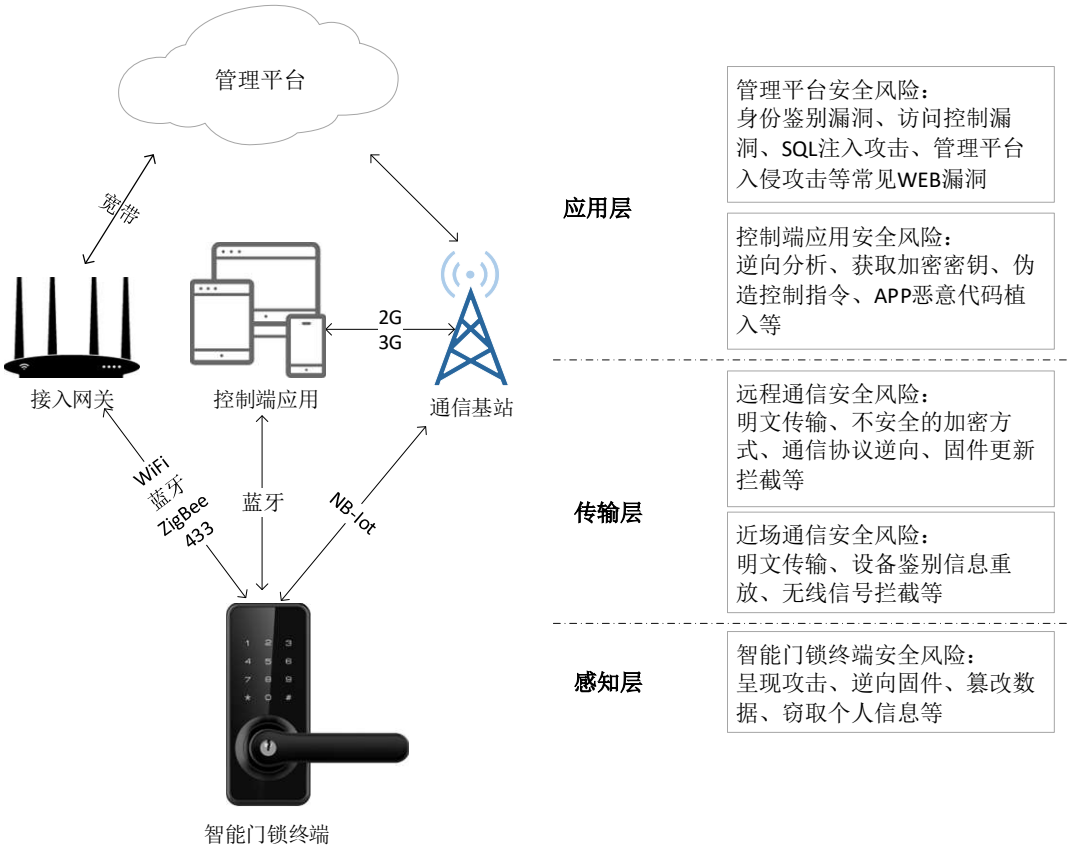

图 A.1 智能门锁安全风险模型

A.2 安全风险分析

A.2.1 智能门锁终端安全风险

A.2.1.1 控制单元及安全模块安全风险

控制单元及安全模块主要面临物理探测攻击、固件攻击、调试接口攻击、拒绝服务、Abuse 攻击、随机数预测、芯片模块通信中间人攻击、强电磁场攻击、安全启动等安全风险。加列项引导语：

a) 物理探测攻击风险

智能门锁在工作时，应用数据会在各个模块之间传输，传输通过各个功能模块间的金属连线实现，攻击者对这些金属连线进行探测、监听，尝试在用户的会话期间或从先前的已经通过身份验证的用户中利用未受保护的残留安全相关数据(如生物识别数据和设置)，以揭示/重建密钥等重要数据。甚至可以对金属连线上传输的数据进行干扰、修改，对智能门锁的电路结构进行物理篡改、操纵(包含故障分析和 IC 逆向工程)，以改变其安全功能(硬件和软件部分)，甚至导致其安全功能模块失效，进而泄漏重要信息。

b) 固件安全风险

设备固件代码恶意篡改攻击威胁，典型方式如植入木马、后门、二次打包应用程序。该风险多发生在固件升级的过程中，攻击者可通过获得固件、解压、分析并进行篡改，最终远程烧录到设备上。攻击者通过在固件中植入恶意代码，可达到获取用户个人信息和控制设备的目的，从而实现持续性影响，甚至可毁坏设备的正常使用。

未对 FLASH 芯片读写进行保护，攻击者可使用 FLASH 芯片相应的编程器获取二进制数据；固件提取也是攻击者进行软件漏洞攻击的基础，良好的固件保护可以缩小攻击面，而针对固件的提取过程可借助错误注入手段实施攻击(电磁、电压)。

c) 调试接口安全风险

攻击者有可能利用控制单元的调试接口，使设备重新进入测试模式，从而获取设备内部关键信息。攻击者有可能使用伪造的身份，获取设备调试接口的控制权，对内部资源进行访问。攻击者也可以使用调试接口刷入改动后的固件，在门锁中植入后门。

d) 拒绝服务攻击风险

攻击者可能通过远程或者本地攻击的方式，使得识别与控制模块对合法授权的用户不能正确识别，导致模块不能正常运行。

e) Abuse 攻击风险

攻击者可能会通过向认证者发送带有无效参数或无效命令的指令来滥用认证者功能。通过智能门锁的响应来推断智能门锁的敏感信息。

f) 随机数预测风险

攻击者可能通过预测随机数的生成，或者通过改变芯片随机数模块的工作条件(如工作电压、温度 等)来影响生成的随机数质量，甚至通过调试接口获取内部产生的随机数。

g) 芯片模块通信中间人攻击风险

芯片模块之间的通信存在中间人攻击风险，攻击者可以试图截取和重放，模仿授权用户的通信过程，从而通过身份认证。

h) 强电磁场攻击

攻击者通过外部的强电磁场发射工具，向门锁发出强电磁波干扰(俗称小黑盒攻击)，电磁波在门锁内部耦合产生电压，可能触发门锁的误动作，包括但不仅限于触发开锁信号，驱动电机，触发 MCU 或识别芯片重启等造成误开锁。

i) 安全启动风险

智能门锁开机或唤醒时未采用启动认证，攻击者可预置加载非授权的攻击代码，绕过操作系统认证鉴权的攻击等。

A.2.1.2 生物识别模块安全风险

生物识别模块主要面临伪造登录及异物混淆识别、敏感信息修改、指纹信息错误接受、指纹识别模块呈现攻击、指纹识别结果篡改、指纹物理残留非法采集等安全风险。

a) 伪造登录及异物混淆识别风险

攻击者可能试图修改截取或重放通信，模仿或生成授权用户的生物特征以伪装成合法用户并登录智能门锁。例如攻击者通过简易指纹膜(导电性或非导电性)对无人值守门锁外

露指纹模块进行表面贴敷，以覆盖少部分指纹传感器，后续如合法用户使用过程中并未发现该指纹膜可能利用算法漏洞实现伪造登录风险，即绕过授权指纹直接开锁。原理为传感器区域表面发生破损或者表面存在异物(如指纹膜等)的情况下，传感器在采集信息时容易采集到夹杂异物特征的信息。在合法用户继续用户使用一段时间后，异物信息有机会伴随正常的用户信息学习进识别模板，异物信息积累到一定程度时会替换掉正常的用户信息，使得识别模块无法正确识别出用户的特征，客户模板被恶意替换。被异物信息替换后的识别模块，由于异物仍旧残留，非正常用户识别时就会出现认假的情况，从而实现识别模块的破解。

此外，2D 人脸技术也存在伪造漏洞，人脸属于弱隐私信息，很容易获取，在打印照片后以特定角度攻击即可实现开锁，或采用相关图像合成软件也可以实现对于所谓活体人脸 2D 检测的欺骗。

b) 敏感信息修改风险

攻击者可能会尝试修改辅助资产，例如生物特征参考或其他与安全相关的系统配置数据。典型攻击包括尝试修改生物特征识别系统用于验证用户的阈值级别，或尝试修改授权用户的生物特征鉴别数据。

c) 指纹信息错误接受风险

由于指纹识别模块的设计缺陷(如指纹传感器的面积、指纹识别算法性能、以及比对判断阈值等方面设计缺陷)，本应拒绝的指纹错误地判断为可以接受，从而使未经过录入的手指可以通过正常的指纹识别流程开启智能门锁。

d) 指纹识别模块呈现攻击风险

不改变指纹识别模块的内部流程，仅通过对指纹传感器输入某些特定图像，使指纹识别模块执行正常的识别流程,但却做出错误的比对判断结果,从而造成非法用户开启智能门锁。

e) 指纹识别结果篡改风险

指纹识别模块需将已录入的指纹图像转换为模板、并存储在非易失性存储器中(例如 Flash 存储器等)，在指纹录入、比对过程中，软件环境的漏洞可能导致相关指纹敏感信息泄露。

针对指纹识别模块中指纹敏感信息的攻击，存在本地和远程两种攻击方式，其中本地攻击，可采用侵入式、半侵入式针对硬件模块或芯片进行攻击；远程攻击，由于智能门锁具备网络通信功能，攻击者可以利用网络协议漏洞远程获取指纹敏感信息，篡改指纹识别算法输出的比对结果，从而使指纹识别功能失效。

如果智能门锁的前面板机械强度不够高，有可能被破拆、钻洞、进而搭线，指纹比对结果传输至主控芯片的链路有可能被实施中间人攻击，即在传输过程中被篡改。

f) 指纹物理残留存在被非法采集风险

智能门锁合法用户的指纹残留存在被非法采集的风险，而被采集的指纹残留可被用于制作假指纹进而非法开启智能门锁。针对残留指纹信息制作假指纹的种类可以分为以下几种：

1) 2D 打印假指纹;
2) 2D 导电硅胶假指纹;
3) 3D 导电硅胶假指纹。

攻击者可以通过一系列的手段采集到识别器上残留的指纹信息，并且通过这些信息恢复用户的指纹，从而实现攻击破解。

A.2.1.3 键盘安全风险

键盘主要面临口令偷窥、覆盖攻击、按键音分析、暴力攻击、口令硬件木马植入、口令云端存储及传输等安全风险。

a） 口令偷窥

智能门锁上的无遮挡键盘在输入口令时，周围环境被安装微型摄像头进行偷窥的风险。

b） 覆盖攻击

攻击者可在键盘上覆盖一层薄膜，以获取用户的开锁口令。

c） 按键音分析

不同按键声音可能不同，存在被窃听泄露口令的风险。

d） 暴力攻击

攻击者可能尝试使用暴力攻击的方法对智能门锁的口令、指纹、钥匙等进行攻击。攻击者通过大量的非法尝试,暴力破解智能门锁的身份验证。口令校验算法应该拥有完备的逻辑，当输入过长的口令，校验算法可以做正确的处理，不会触发崩溃，而使得程序出现异常。

e） 口令硬件木马植入

缺少主动探测的防拆机制，未采用工业设计手段保护硬件安全，存在安装物理木马设备窃取口令的风险。

f） 口令云端存储及传输

将用户口令信息存储在云端可能带来更大的信息安全隐患，如网络攻击或传输过程中被截取等，因而对口令的存储与传输均有极高安全要求以抵抗黑客攻击。

A.2.1.4 IC卡及读卡器安全风险

部分拥有 NFC 功能的智能手机为方便用户推出门禁 IC 卡复制功能，该功能降低了对于低成本非 CPU 卡的复制门槛和技术成本。

a） 低频卡复制

低频卡内部因只保存一串唯一的序号,通过读写器读取序号写入空白 ID 卡即可完成非法复制。

b） 高频卡复制

当读卡器仅识别高频卡的 UID 作为身份识别信息时，非法用户可通过复制 UID 完成对 IC 卡的复制；使用 UID 及密钥认证扇区作为身份识别信息时，当高频卡存在以下问题时可被复制：

1） 采用了默认口令；

2） 密钥长度小于 48 比特造成破解时间较短；

3） 采用了可被预测的伪随机算法生成密钥。

c） IC卡信息推导

IC 卡关键验证数据要充分熵化，避免通过门锁型号、批号、出厂时间等外部信息推断出关键验证数据，也要避免通过同型号，不同智能门锁关键验证数据可以推断出其他智能门锁关键验证数据的情况。

d） IC卡暴力攻击

IC 卡鉴别要设置尝试次数，防止遍历 ID 等暴力破解攻击。

A.2.2 通信协议攻击安全风险

A.2.2.1 蓝牙通信安全风险

蓝牙通信主要面临配对连接、鉴权认证、链路通信等安全风险。

a） 配对连接

由于智能门锁进行蓝牙配对时，可能采用不同的蓝牙配对机制，当其中一方的蓝牙配对协议安全性较差或因为用户选用了简单的或不安全的蓝牙配对方式(如 PIN 码和 Just works 方式)，配对过程容易被分析或破解。

b） 鉴权认证

不同版本蓝牙协议鉴权认证方式不一样，有的鉴权认证方式比较简单，容易被第三方截获或者破获；相同蓝牙协议存在不同的鉴权认证机制，这些鉴权机制的安全性不一，也容易造成安全隐患；

c） 链路通信

由于蓝牙通信是无线通信，因此通信的数据是可以被侦听、伪造或干扰的，因此链路通信风险体现在几方面：

1） 同频干扰(虽然有跳频机制，但是跳频机制是在连接时就可以获取的)，造成通信成功率降低或瘫痪；
2） 因不启动链路层加密，数据直接明文传输，这样数据可以被直接截获，或者数据被第三方伪造，插入攻击者的数据；
3） 链路数据加密的方式不一致，因此使得数据加密的安全性不一样，也造成数据攻击的漏洞，被攻击者截获数据；
4） 蓝牙芯片的加密算法运行环境防护较弱,攻击者可以通过功耗分析等手段窃取加密密钥，破解加密的通信数据；
5） 没有对关键传输信息进行签名，每次使用相同的密钥、相同的加密方式、发送相同的信息，无法抵御重放攻击。

A.2.2.2 Zigbee 通信安全风险

Zigbee 通信主要面临鉴权认证、链路通信等安全风险。

a） 鉴权认证

在 ZHA1.2 及之前的版本中，Zigbee 有一个统一的 KEY 来保证不同厂家的设备能加入到同一个网络。在设备入网时，使用这个 KEY 来加密 Network Key，这时第三方能够截获或者破获得到 Network Key；在 Zigbee3.0 中,使用 Install Key 的方式来修正了这一问题，但需要通过别的途径来传输 Install Key,可能会有被截获的风险。

b） 链路通信

由于 Zigbee 通信是无线通信，因此通信的数据是可以被侦听、伪造或干扰的，因此链路通信风险体现在几方面：

1） 同频干扰，造成通信成功率降低或瘫痪；
2） 启用链路层加密，但仅采用 AES-128 算法加密，密钥位数及强度不够；
3） Zigbee 芯片的加密算法运行环境防护较弱，攻击者可以通过功耗分析等手段窃取加密密钥，破解加密的通信数据。

A.2.2.3 Wi-Fi 通信安全风险

Wi-Fi 通信面临被动侦听、KRACK 攻击等安全风险。

a） 被动 Wi-Fi 侦听

攻击者主动架设自己的 AP，SSID 命名为具有引诱性的 SSID，吸引主动连接。被攻击设备连接上该 AP 后可以正常上网，但是所有报文都会在攻击者的 AP 上中转，被攻击者即使使用 HTTPS/SSL 协议，攻击者仍然能够发起多种攻击，例如：中间人攻击等。

在中间人攻击中，攻击者可以通过技术手段模仿连接的 AP 向设备发送 IEEE 802.11 协议里的 De-Association （解除关联)报文，设备就会被迫与正常的 AP 断开连接。攻击者会通过一系列手段将设备引导到他自己建立的 AP 上，攻击过程中，设备无感知，期间始终可以正常上网，但是已经被中间人攻击。

b） KRACK 攻击

KRACK(口令重置攻击，Key Reinstallation Attacks)是基于Wi-Fi的WPA2/WPA保护协议本身存在的缺陷，目前，除了禁用Wi-Fi以外，针对协议本身没有任何有效的防护方案。

WPA2/WPA是目前全球应用最广的Wi-Fi数据保密协议，根据WPA2/WPA的原有设计，一个密钥只能使用一次,通过操纵重放加密握手消息(即:记录设备与Wi-Fi路由器间的通信数据，并重新发送出去)的动作，可令已有密钥被重复使用。由此，攻击者就获得了一个万能密钥，利用这个万能密钥，攻击者可以攻破WPA2协议，窃听Wi-Fi通信数据，破译网络流量、劫持链接、将内容注入流量中。

KRACK漏洞并不是某一个Wi-Fi设备本身的问题，也不是换口令就能解决的问题，而是安全保护机制本身存在的缺陷，绝大多数Wi-Fi设备都会受到影响，包括微软、安卓、苹果及基于Linux开发的设备。KRACK攻击对Wi-Fi设备本身并不造成影响，它绕过登录系统直接截取通信数据， KRACK攻击者无需掌握口令，只要靠近Wi-Fi设备，即可通过KRACK攻击来获取或篡改Wi-Fi通信内容。

A.2.3 控制端服务安全风险

控制端服务面临的安全威胁众多，包括各类程序病毒、木马、间谍软件、劫持攻击等软攻击及远程攻击手段，以获取账户的 ID 和口令，获取设备的访问权，控制权等，并侵入终端设备硬件平台、操作系统，窃取核心代码或者算法，破解密钥、加密算法，挖掘控制协议、后台交互逻辑漏洞等。进而实现暴露系统漏洞、对系统后台进行攻击、控制系统、劫持/控制设备、获取用户信息/机密数据等操作。

a) 操作系统

操作系统是应用及业务执行的基础，为其提供稳定安全的执行环境。黑客对系统底层的劫持、伪装、篡改以出现非用户意愿的行为的执行，同时，操作系统也面临自身升级时的风险挑战。

b) 控制安全

智能门锁可与外围设备(如手机)连接，并授权合法设备对其进行操控。黑客可对通过对两侧设备的侵入，以窃取账号、口令、数据等。所以，需确保连接和数据传输安全保护，确保连接开启/关闭受控，连接建立的认证与授权、连接状态标识、数据传输安全保护。

c) 业务应用安全

业务应用安全风险主要来源于恶意攻击、敏感行为控制，以产生非用户意愿的行为，或虚假的设备状态信息。同时要甄别是否存在业务应用漏洞，无未经授权的修改、删除、窃取用户数据的行为。

d) 数据安全

用户数据分为涉及设备合法授权及操作的信息，如账号、密钥、口令等；以及用户隐私数据，如使用设备的时间、地点、频次等，可溯源用户行为及人身安全的尤为敏感。黑客通过控制设备，链路连接等方式以监听敏感数据，甚至是篡改，伪造用户数据。所以，终端需保证用户数据的安全存储，确保用户数据不被非法访问、不被非法获取、不被非法篡改。

A.2.4 管理平台安全风险

管理平台的安全风险是指可能对资产或组织造成损害事故的潜在因素。管理平台的安全风险一般为外部风险，主要包括如下：

a) 身份假冒

此风险的主体主要为非法用户，也有少量的合法用户，风险的客体为所有物理资产、软件资产和数据资产。此风险主要是合法用户冒用别人的身份或账号进行一些合法操作，或者非法用户盗用合法用户身份或账号进行非法操作，这两种情形在冒用账号方面发生可能性

比较高。

b） 敏感信息泄漏

此风险的主体为非法用户，也有少量合法用户，主要是蓄意盗取敏感数据或泄露应该保密的信息，风险的客体为软件资产和数据资产。这些非法用户利用社交等手段获取系统软件或应用软件的配置数据，以便为后面的破坏做好基础，或者直接骗取业务敏感数据，此风险较为隐蔽，利用的手段较多。

c） 数据篡改

此风险的主体为非法用户，客体为数据资产。篡改是在未经授权的情况下更改或删除资源。数据在传输中(以物理或电子方式)和存储时都会受到此风险。例如，未受保护的数据包可被截获和修改，或者数据可因为攻击者利用缓冲区溢出执行的恶意代码而损坏。

d） 拒绝服务

此风险的主体为非法用户，主要是故意破坏的攻击者，风险的客体为软件资产。此风险一般是内部的破坏者针对内部应用系统的有效攻击方式，发生可能性较大。外部的攻击者针对公开服务的各种系统都有可能进行攻击。

e） 数据窃听

此风险的主体为非法用户，风险的客体为软件资产和数据资产。非法用户通过窃听手段窃取系统软件和应用软件的系统数据及敏感的业务数据，为了达到攻击和入侵系统的目的，攻击者一般都会进行这方面的尝试。

f） 恶意代码

此风险的主体可以视为系统问题，也可以看作系统外部人员的恶意行为。但是恶意代码往往不是有针对性的行为，可能是其它软件或系统漏洞引发的结果。风险的客体为软件资产和信息资产，目前有些恶意代码也可能威胁硬件资产的安全。系统感染病毒的可能性较多，但也有可能被非法用户利用漏洞安装恶意代码，此风险的可能性与系统的防病毒体系建设和安全漏洞的严重程度有关。

g） 不合理的配置

此风险的主体为非法用户，主体为操作系统、应用软件和 TCP/IP 协议。大多数系统软件和应用软件为了方便用户，初始安装结束之后，存在一些默认的用户名、口令和开放的服务端口。这些配置往往会被攻击者利用，造成网络瘫痪或机密被窃取。另外，TCP/IP 某些协议存在一些漏洞，非法用户可以利用此漏洞进行入侵系统，获取管理员的权限。这些风险发生的可能性适中。