电 信 终 端 产 业 协 会 标 准

TAF-FG1-AS0030-V1.0.0:2019

智能门锁信息安全技术要求和评估方法

Information Security Technical Requirement and Evaluation Method on Smart Gate Lock

2019-04-23 发布　　2019- 04-23 实施

电信终端产业协会　　发 布

目 次

前　　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、中国电信终端公司、中移物联网有限公司、北京鼎合思锐软件技术有限公司、深圳市纽创信安科技开发有限公司、上海果通通信科技股份有限公司、郑州信大捷安信息技术股份有限公司、紫光同芯微电子有限公司、上海掌御信息科技有限公司、北京百度网讯科技有限公司、意法半导体、深圳联亨智云智能科技有限公司

本标准主要起草人：国炜、潘娟、耿炎、赵峰、路晔绵、王海兰、樊俊锋、孙景峰、李勋宏、梁松涛、尹文基、陈珊、黄钧、李笑如

引　　言

随着互联网技术、云技术、高端制造技术的开发与应用，智能家居行业油然而起。而这其中，智能门锁堪称是智能家居的入口级产品，乃至各大企业都盯住了这块巨大的市场蛋糕。然而在市场发展初期，由于缺乏良好的市场规则、以及有效的市场监管措施，更是缺少统一的产品互联和安全标准，使这些智能产品良莠不齐地出现在消费者的日常生活中，在给消费者带来方便的同时，也相继带来了很多安全问题。

本标准从信息通信安全的角度制定智能门锁信息安全技术要求和评估方法。

智能门锁信息安全技术要求和评估方法

1 范围

本文档规定了智能门锁信息安全技术要求和评估方法，原则上仅在协会内部使用，为协会开展智能门锁安全评估提供技术依据。本文档是评估实验室进行智能门锁安全测试的指南，也可以供认证产品的生产商使用。

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，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语、定义和缩略语

3.1 缩略语

4 智能门锁结构和功能架构

4.1 智能锁整体架构

智能门锁的整体应用架构根据现有技术方案可分为2种，一种是连接网关通信结构，一种是蜂窝通信结构，如NB-IOT。两种应用架构中主要包括智能门锁本地端，智能门锁云管理平台和管理客户端三大组成部分，整体架构图如下：

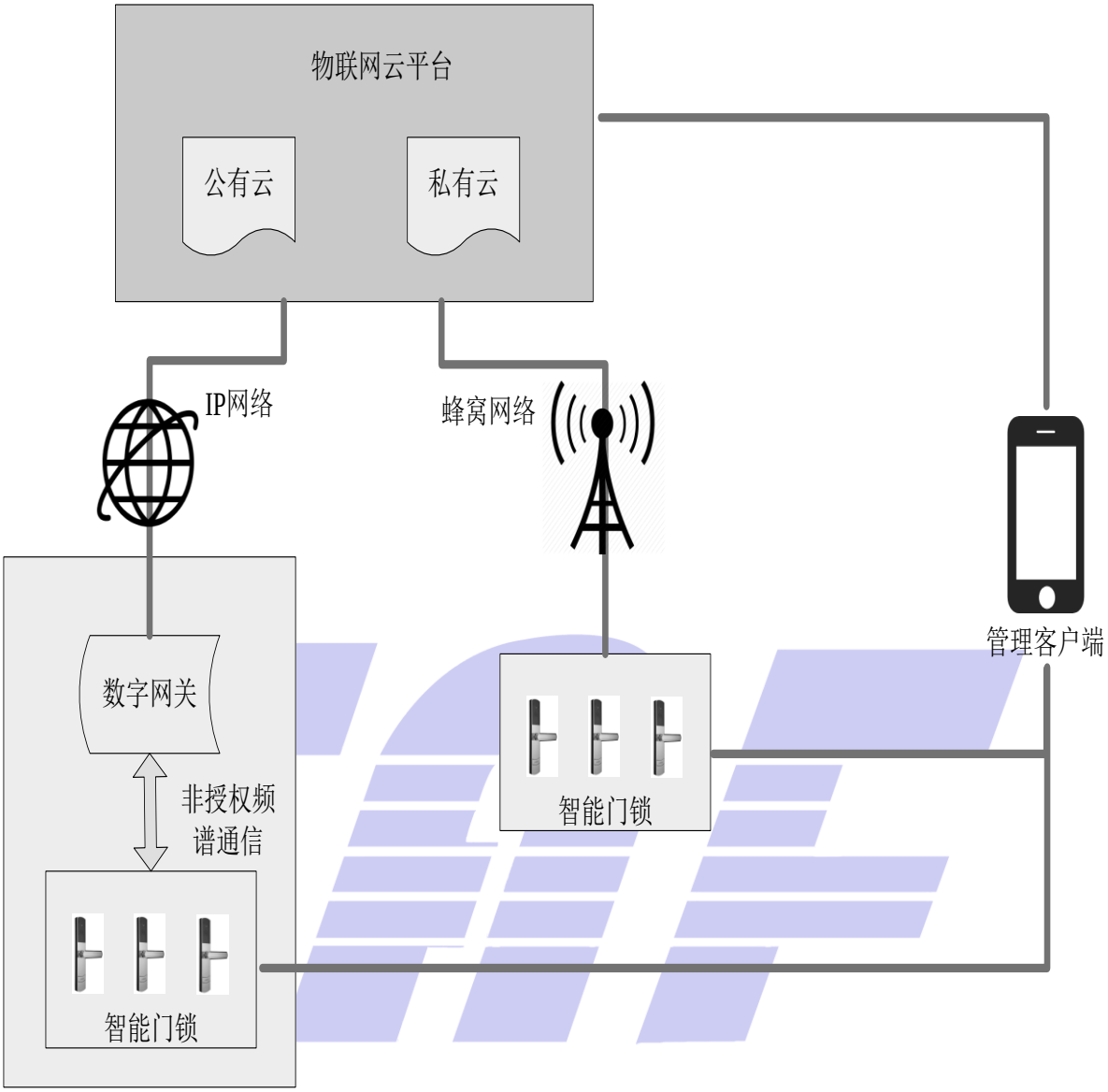

图1 智能门锁应用架构

智能门锁本地端由前面板、锁体和后面板三部分组成，其中前面板包含众多复杂的电子器件，如电机、主控电路板、显示屏、信息采集模块（如密码输入界面、指纹识别模块）、把手和滑盖等元器件，它一般为面向门外的开锁界面；锁体结构包括机械锁体部分、电机和锁芯部分，后面板包含了通讯模块如WIFI、蓝牙、Zigbee、NB-IoT等、反锁控制键、电池槽、后把手。

智能门锁云管理平台通过网络将管理客户端和智能门锁本地端进行连接并保证其传输安全，同时承担管理客户端对本地端接入、控制、授权等操作的认证功能，以及对所有操作的日志和审计功能。

管理客户端为用户提供能够通过物联网云平台对智能门锁本地端进行远程操作的接口，其主要应对其临时存储或者持久存储的数据进行保护，并对智能门锁云管理平台的数据传输进行保护，同时采用一定的安全机制保障自身安全。

4.2 智能门锁本地端功能

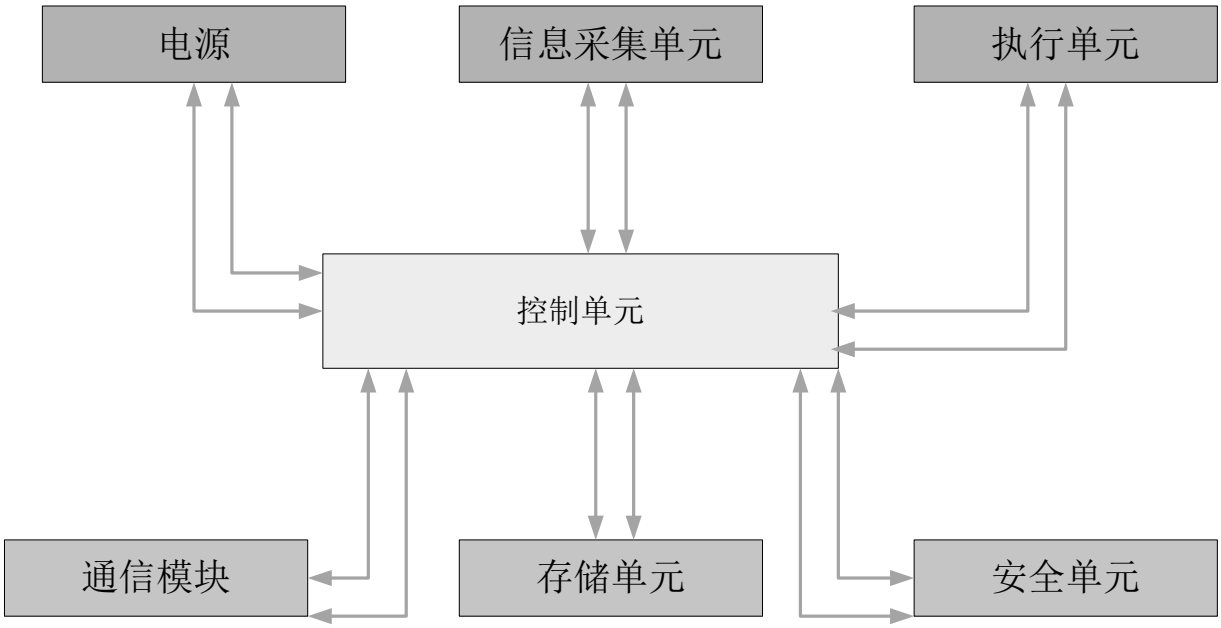

图 2 智能锁本地端功能架构图

如图2所示，智能门锁本地端包含的主要功能模块如下：

信息采集单元：通过该单元采集能够驱动本地端机械锁体部分的信息，包括密码信息、生物识别信息。该信息要有唯一性、安全性、方便性、兼容性、广泛性等特点。

通信模块：通过该单元将锁体上的信息如状态信息、开关信息等，借助通信网关或者其它网络设备传递到智能门锁云管理平台，同时反向可接收云管理平台传递的控制信息，启动本地端的控制单元完成机械锁体部分的控制。

存储单元：内部存储秘钥、固件、应用数据的物理单元，如智能门锁的主控秘钥、过程秘钥、加密秘钥、解密秘钥、临时秘钥、认证秘钥都需要存储在该物理单元内。

安全单元：实现智能门锁本地端用户如指纹、密码、人脸识别、虹膜识别、指静脉等多种生物特征验证凭据的身份认证，以及智能门锁云管理平台的控制指令有效性验证，认证结果将反馈至控制单元。

执行单元：通过接收控制单位发送的指令，完成对智能门锁本地端机械锁体部门的动作。

控制单元：作为智能锁的核心功能模块，起到各模块间信息协同与交互的作用。

除此之外，智能门锁还包括机械和锁芯部分。对这两部分的安全技术要求不在本标准的规定范围内。

5 总体安全目标

5.1 安全风险

5.1.1 本地安全风险

- 用户信息被窃取
- 生物特征信息被窃取
- 固件被非法读取或篡改

- 开锁 PIN 码被提取
- 门卡被复制
- 控制命令被重放
- 控制命令被伪造

5.1.2 远程安全风险

- 远程非法登陆智能门锁云管理平台
- 服务器远程用户提权
- 固件非法升级
- 控制命令被重放
- 控制命令被伪造
- 智能门锁云管理平台被拒绝服务攻击
- 用户信息被远程截取
- 生物特征信息被远程截取

5.2 安全目标

5.2.1 本地安全目标

设备在固件存储、固件升级等方面应有足够的防护，防止攻击者通过提取固件、分析固件、操控固件非法操控智能门锁设备。

智能门锁在开关锁具的令牌、密码、生物特征识别、近场控制命令等方面应具有足够的安全防护，防止攻击者通过攻击上述模块非法操控智能门锁设备。

智能门锁应在软硬件设计上具有安全防护，以防止用户提权、生命周期修改、设备工作模式修改等非法操作。

5.2.2 远程安全目标

智能门锁与智能门锁云管理平台、智能门锁与管理客户端、智能门锁与控制网关之间应具有足够的通信加密机制，以防止控制命令重放和伪造、远程用户提取。

智能门锁与智能门锁云管理平台、智能门锁与管理客户端、智能门锁与控制网关之间应具备验证机制，以防止非法远程登录、非法远程固件操控。

5.2.3 隐私数据安全目标

智能门锁应具有足够的防护措施，以防止用户的隐私数据在设备端、通信过程中泄露。

智能门锁作为一种安全设备，应确保只有合法用户通过设定的方法控制，并确保用户隐私数据的安全。

智能门锁应具有足够的安全防护措施来应对包括本地破解、远程非法控制、用户隐私数据泄漏，并通过相应的攻击测试。

6 安全功能要求

6.1 控制单元

控制单元应支持智能门锁的防拆保护机制，且当检测到外部拆解门锁的行为时，控制单元应给出报警信息，并采取适当的行为保护锁内信息的安全。

控制单元应支持智能门锁工作环境检测机制，且当检测到门锁的工作环境（温度、电源电压、工作电流、电磁脉冲等）超过门锁正常工作范围时，控制单元应给出报警信息，并采取适当的行为保护锁内信息的安全。

控制单元应具备足够的安全防护能力，保证自身在受到干扰（温度、电源电压、电磁脉冲等）的情况下能够保持安全的工作状态。

控制单元应支持敏感信息的安全传输、安全存储和安全使用。

6.2 信息采集单元

对于具备生物识别开锁功能的智能门锁，生物采集模块应支持活体检测能力。

对于使用信息识别卡开锁功能的智能门锁，信息识别卡应具备防复制能力；且应采用口令或密码算法对信息识别卡鉴别信息读写等操作设置控制权限，限制非授权的信息识别卡访问。

6.3 通信模块安全

6.3.1 通信模块的通用安全要求

1) 通信模块应使用加密算法和完整性保护算法保证通信的加密，避免侧信道攻击。

6.3.2 蜂窝通信模块的安全要求

1) 蜂窝通信模块需要具备不可更改的设备IMEI号，以便网络侧可利用IMEI号实现机卡互锁功能。
2) 蜂窝通信模块应具备双向鉴权能力，防止伪基站攻击，防止附着一个不可信的网络上。根据目前网络部署情况，建议采用3G/4G/NB-IoT/eMTC等网络，避免使用2G网络。
3) 当安全元件同时作为eSIM功能时，蜂窝通信模块需要支持转发安全应用层数据能力，以便向MCU提供应用层的身份识别和数据加密、完整性校验功能。

6.3.3 蓝牙模块的安全要求

1) 蓝牙模块应支持加密传输。
2) BLE 4.2版本及以上的模块应使用LE Secure Connections功能。

6.3.4 ZigBee 模块安全要求

1) 应使用访问控制模式或安全模式进行通信。
2) 当使用访问控制模式时，通过访问控制列表限制非法节点获取数据；
3) 当使用访问控制模式时，ACL采用预置的方式，且使用安全存储机制。
4) 当使用安全模式时，采用AES 128位加密算法进行通信加密，同时进行完整性校验。
5) 当使用安全模式时，密钥采用预置或预置SALT+衍生的方式，预置的密钥或者SALT应使用安全存储机制。

6.3.5 433MHz 无线、WIFI 模块的安全要求

应符合6.3.1所规定的要求。

6.4 存储单元

6.4.1 概述

智能锁使用的存储单元包括RAM、ROM和Flash存储。

- RAM：用于系统启动后的应用程序、数据的保存，掉电后复位；
- ROM：用于保存系统启动程序、系统软件，不可擦写；
- Flash：用于保存系统配置、关键业务数据的持久化、日志数据，掉电保持，可重复擦写；

6.4.2 RAM 存储安全

对RAM存储单元，应该采用统一的内存管理机制，划分安全区域和非安全区域，分别存放敏感数据和非敏感数据。敏感数据又称隐私数据，如用户身份信息、密码、位置等与用户相关的数据，而其它非涉及用户相关的数据为非敏感数据。对涉及安全操作的软件模块，可以向内存管理服务申请安全区域的内存以及非安全区域的内存；对涉及非安全相关的模块，只能向内存管理服务申请非安全区域的内存。

6.4.3 ROM 存储安全（可选）

对ROM存储单元，本身属于不可擦写存储，存储的数据不需要进行额外的保护。但系统启动代码在加载Flash存储单元的程序时，应进行签名验证。系统启动代码还要防止电磁攻击，避免寄存器错乱导致的异常行为。

6.4.4 Flash 存储安全

对于Flash存储单元，存储的内容包括固件代码和数据。

- 固件代码：应对固件代码采用签名验证，且固件代码应具有反逆向保护。
- 固件更新FOTA：空中更新的固件代码应该采用代码签名机制来验证代码的完整性和可靠性，且应具有防回滚功能。
- 数据：敏感数据在存储时应采用加密存储，且安全存储的密钥可以由硬件安全单元衍生。

6.5 安全单元

6.5.1 概述

智能门锁如具备硬件密码模块或硬件安全单元(Secure Element)，则智能门锁使用指纹、虹膜、人脸、指静脉（不限于以上方式）等生物识别特征进行身份识别时，应采用密码模块对相关敏感信息进行加密存储；远程、近端等传送给智能门锁系统的关键信息（如控制信息、配置信息等）应进行签名验证。

6.5.2 抗攻击防护

硬件密码模块或安全单元应具备安全防护机制，能够防止物理攻击、侧信道攻击、故障注入攻击等静态和动态的攻击。且需要对芯片工作环境进行监控，当芯片遭受可疑的攻击时，产生告警信息；对其内部总线以及存储器等重要敏感电路部分增加物理保护层，以阻止入侵者利用探针等手段窃取信息；通过设计随机振动的电源提高抗功耗分析攻击的能力。

6.5.3 密钥管理安全

硬件密码模块或安全单元支持多级密钥离散的机制，智能门锁各级发卡方在卡片主控密钥和应用主控密钥的控制下装载应用和密钥。

硬件密码模块或安全单元主控密钥是卡片的控制密钥，初始值由安全单元生产商写入，由发卡方替换为发卡方的卡片主控密钥。卡片主控密钥的更新在发卡方自身的控制下进行。

硬件密码模块或安全单元主控密钥的访问控制可通过外部认证操作实现，也可通过安全报文的方式实现。发卡方必须在安全单元主控密钥的控制下完成装载应用主控密钥和更新卡片主控密钥。

应用层密钥包括应用主控密钥、应用维护密钥、应用工作密钥、应用数据。应用主控密钥是在安全单元主控密钥控制下写入的。发卡方必须在应用主控密钥的控制下完成装载应用维护密钥、应用工作密钥和更新应用主控密钥。

硬件密码模块或安全单元应提供密钥分散、数据加密和完整性校验功能。应支持国际主流的标准加密算法，若支持国密算法，则应符合国家密码管理机构的相关规定。

6.6 传输安全

6.6.1 传输安全通用技术要求

智能门锁的信息传输安全涉及智能门锁、控制终端、智能门锁云管理平台的数据处理单元之间的数据安全传输。智能门锁传输安全泛指采用密码技术在智能门锁、控制终端、云管理平台的数据处理单元之间保证数据传输的完整性、机密性和抗重放攻击。传输安全不涉及智能门锁内部数据传输的安全要求。

6.6.2 数据传输完整性技术要求

智能门锁应用的各个执行主体之间在进行数据传输时，应采用数据完整性校验机制保证传输数据的完整性。

a) 智能门锁各个执行主体之间在进行数据传输时，除传输数据主体之外应附加用于对数据进行完整性校验的校验信息；

b) 智能门锁各个执行主体之间在进行数据传输时，可根据传输不同分类级别的数据采用不同的数据校验方法；

c) 智能门锁各个执行主体之间在传输控制指令、管理数据、隐私数据、重要业务数据等重要数据时，可采用密码机制保证数据传输完整性，采用的密码机制应支持国际主流的标准加密算法，若支持国密算法，则应符合国家密码管理机构的相关规定；

d) 在检测到传输数据的完整性遭到破坏时，应采取措施恢复或重新获取数据。

6.6.3 数据传输机密性技术要求

智能门锁应用的各个执行主体之间在进行数据传输时，应采用密码机制保证传输数据的机密性。

a) 智能门锁各个执行主体之间在进行数据传输时，应采用密码机制对传输数据进行加密；

b) 智能门锁各个执行主体之间对于重要数据、鉴别信息和重要业务数据的传输，应采用有一定强度的加密算法对数据进行加密；

c) 智能门锁各个执行主体之间在传输加密数据时，应采用一次一密的加密传输方式；

d) 智能门锁各个执行主体之间传输数据时的加密算法，可采用国产密码算法；

e) 智能门锁各个执行主体之间在进行数据传输时，若涉及密钥管理，密钥管理策略应能够解决周期密钥更新、密钥撤销和密钥分发等问题。

6.6.4 数据传输抗重放技术要求

智能门锁应用的各个执行主体之间在进行数据传输时，应采用一定的机制保证传输数据的抗重放攻击。

a) 智能门锁各个执行主体之间在进行数据传输时，应采用机制防止数据包或报文的重排或重放；

b) 智能门锁各个执行主体之间在进行数据传输时，可使用序列码或时间戳实现抗重放攻击；

c) 智能门锁各个执行主体之间在进行数据传输时，可在数据中加入与当前事件有关的一次性随机数。

6.7 安全认证

6.7.1 安全认证通用技术要求

智能门锁应用中各个执行主体之间应具备认证鉴别机制，各个执行主体之间可采用不同的身份认证和鉴别机制。

6.7.2 接入认证

智能门锁应用的各个执行主体之间应采用身份认证或鉴别机制实现接入认证。

a) 智能门锁接入云管理平台时，应对智能门锁与云管理平台之间采用身份认证及鉴别机制；

b) 控制终端接入云管理平台时，对云管理平台与控制终端之间应采用双向身份认证及鉴别机制；

c) 智能门锁与控制终端之间，应建立基于身份的双向认证机制；

d) 接入认证失败时，云管理平台应支持以下失败处理：

能终止智能门锁或控制终端端接入认证超时的当前会话；

能终止智能门锁或控制终端规定次数认证失败的接入会话的尝试。

6.7.3 控制认证

控制终端与智能门锁之间应建立控制认证鉴别机制。

a) 控制终端与智能门锁之间应建立基于数字证书的双向身份认证机制；

控制终端与智能门锁之间应保证只有认证通过的控制终端可控制相应的智能门锁；

控制终端与智能门锁之间应保证只有认证通过的智能门锁可接收并执行相应的控制指令；

b) 控制认证失败时，应终止控制终端对智能门锁的控制请求。

6.7.4 授权认证

云管理平台用于建立智能门锁与控制终端之间的授权认证机制，通过云管理平台实现控制终端与智能门锁之间的信息绑定。

a) 云管理平台向控制终端进行授权时，应建立云管理平台与控制终端之间的认证机制；

b) 云管理平台应支持授权控制终端仅可访问被授权绑定的智能门锁，并能阻止非授权的控制终端的访问请求；

c) 云管理平台在向不同级别的控制终端用户进行授权时，应采取不同级别的授权权限；

d) 云管理平台应支持对控制终端与智能门锁之间的绑定关系的修改、解除；

e) 云管理平台应支持授权控制终端访问历史的智能门锁数据。

6.8 管理客户端安全

6.8.1 访问控制

客户端APP应能对访问者进行验证，只接受通过认证的用户的访问，同时应对敏感数据进行访问权限控制。

6.8.2 数据安全保护

应加密存储敏感数据，敏感数据存储路径应设置严格的访问控制机制，避免数据泄露。用于加密的密钥应妥善保存，避免被直接获取。

应禁止日志数据包含与用户数据相关的数据。

6.8.3 反逆向保护

应采取代码混淆、加壳等防护措施，实现客户端APP反编译保护。

6.8.4 反盗版保护

应采取签名机制，防止客户端APP被重打包。

6.8.5 防篡改攻击

应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。

7 测试内容和评估方法

7.1.1 测试内容与安全分级

测试内容将全部覆盖4.2节所定义的功能模块，以及对应的第6章所规定的安全功能要求。同时，将这些安全功能要求按照级别由低到高被包含在不同的一级、二级、三级里。具体内容见表1。

表1 测试内容和安全分级

测试单元	测试项	一级	二级	三级
控制单元	控制单元应支持门锁的防拆保护机制	√	√	√
	控制单元应支持门锁工作环境检测机制	√	√	√
	控制单元应具备自身的安全防护能力		√	√
	控制单元应支持敏感信息的安全传输、存储和使用			√
信息采集单元	生物采集模块应支持活体检测能力		√	√
	信息识别卡应具备防复制能力；且应采用口令或密码算法对信息识别卡鉴别信息读写等操作设置控制权限，限制非授权的信息识别卡访问。	√	√	√
通信模块安全	通信应支持加密算法和完整性保护算法	√	√	√

	蜂窝通信模块应具备 IMEI 号	√	√	√
	蜂窝通信模块应具备双向鉴权能力	√	√	√
	当安全芯片具备 eSIM 功能时，蜂窝通信模块应支持转发安全应用层数据能力，以便向 MCU 提供安全应用层的身份识别、数据加密、完整性校验功能（条件性支持）			√
	蓝牙模块应支持加密传输	√	√	√
	BLE 4.2 版本及以上的模块应使用 LE Secure Connections 功能		√	√
	ZigBee 模块应使用访问控制模式或安全模式通信	√	√	√
	在访问控制模式下，通过访问控制列表限制非法节点获取数据	√	√	√
	在访问控制模式下的 ACL 采用预置方式，并使用安全存储机制	√	√	√
	在安全模式下，采用 AES 128 位加密算法，同时进行完整性校验		√	√
	在安全模式下，密钥采用预置或预置 SALT+衍生方式，密钥使用安全存储机制		√	√
存储单元	在加载系统启动代码时，应进行代码的完整性和可靠性验证（系统安全启动）		√	√
	固件在写入时应进行代码签名验证	√	√	√
	固件代码应进行反逆向保护		√	√

	敏感数据在存储时应采用加密存储	√	√	√
	通过 OTA 更新的固件代码应采用签名验证,且应具有防回滚功能		√	√
	对 RAM 存储单元，应采用内存管理机制来划分安全区域和非安全区域对敏感数据以及非敏感数据的存储		√	√
传输安全	各执行主体之间进行数据传输时，应保证数据传输的完整性	√	√	√
	在检测到传输数据的完整性遭到破坏时，应采取措施恢复或重新获取数据	√	√	√
	各执行主体之间进行数据传输时，应保证数据传输的机密性	√	√	√
	各执行主体之间进行数据传输时，应具备抗重放攻击能力。	√	√	√
安全认证	各执行主体之间应采用身份认证或鉴别机制实现接入认证	√	√	√
	控制终端与智能门锁之间应建立控制认证鉴别机制	√	√	√
	控制终端与智能门锁之间应建立控制认证鉴别失败时，应终止控制终端对智能门锁的控制请求	√	√	√

	云管理平台应支持授权控制终端仅可访问被授权绑定的智能门锁，并能阻止非授权的控制终端的访问请求	√	√	√
	云管理平台在向不同级别的控制终端用户进行授权时，应采取不同级别的授权权限	√	√	√
	云管理平台应支持对控制终端与智能门锁之间的绑定关系修改、解除	√	√	√
	云管理平台应支持授权控制终端访问历史的智能门锁数据	√	√	√
管理客户端安全	客户端 APP 应具有用户身份认证机制	√	√	√
	客户端 APP 应对敏感数据进行访问控制	√	√	√
	客户端 APP 应加密存储敏感数据，且加密密钥避免被直接获取	√	√	√
	应禁止日志包含用户敏感信息	√	√	√
	客户端 APP 应采取代码混淆	√	√	√
	客户端 APP 应采取加壳防护措施		√	√

	客户端 APP 应具备签名机制	√	√	√
	应对程序的完整性进行校验，防止篡改攻击		√	√
安全单元	安全单元应能够防止物理攻击、侧信道攻击、故障注入攻击			√
	当安全单元遭受到如上硬件物理攻击时，应产生告警信息			√
	安全单元应具备密钥初始写入、密钥存储、密钥衍生、密钥管理机制			√

7.1.2 评估方法

评估方法采用基于黑盒的功能性验证与渗透性测试。申请厂商需要提交简要的功能说明文档和被测样品。实验室测试人员将依照功能说明文档对产品的功能进行复合型验证，同时测试人员将在一定时间内针对产品的功能涉及渗透性测试环境、配置，并开展一定时间内的渗透性测试。

根据功能性验证和渗透性测试，对智能门锁产品进行分级评定。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容
2018.7.19	V0.1	全文格式
2018.10.23	征求意见稿	全文格式
2018.11.30	送审稿	全文格式
2019.3.4	报批稿	全文格式

附　录　B
（资料性附录）
附录

参 考 文 献