ICS 35.240.01
L67

团　　体　　标　　准

团体标准编号

《智能门锁自动控制模块技术要求》

Technical Requirements for smart lock auto-control module

（征求意见稿）

本稿形成日期：2020-05-20

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：

智能门锁自动控制模块技术要求

1 范围

本标准规定了智能门锁自动控制模块系统架构、主控模块、安全模块、按键模块、蓝牙模块、读卡模块、通信模块和生物特征识别模块等。

本标准适用于智能门锁的设计、制造和应用等。

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/T 18336.3-2015 信息技术 安全技术信息技术安全评估准则 第3部分：安全保障组件

GB/T 38556-2020 信息安全技术 动态口令密码应用技术规范

GA 450-2013 台式居民身份证阅读器通用技术要求

GA 1153-2014 手持式居民身份证阅读器

GM/Z 0001-2013 密码术语

GM/T 0005-2012 随机性检测规范

GM/T 0008-2012 安全芯片密码检测准则

GM/T 0021 动态口令密码应用技术规范

JR/T 0118 金融电子认证规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能门锁 smart lock

采用信息技术控制的锁具及相关系统。

3.2

智能钥匙 smart key

通过密钥认证、生物识别、图形或数字密码等数字化认证方式，实现与智能门锁终端进行安全交互认证完成开锁功能的媒体。

3.3

安全模块 security module

含有密码算法、安全功能，可实现密钥管理机制的相对独立的软件、硬件、固件或其组合。

[参考GM/Z 0001-2013，2.1]

3.4

密钥 key

控制密码算法运算的关键信息或参数。

[参考GM/Z 0001-2013，2.63]

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）

APP 应用（Application）

BLE 低功耗蓝牙（Bluetooth Low Energy）

COS 芯片操作系统（Chip Operate System）

CPU 中央处理单元（Central Processing Unit）

CRC 循环冗余校验（Cyclic Redundancy Check）

DES 数据加密标准（Data Encryption Standard）

3DES 三重数据加密标准（Triple Data Encryption Standard）

DTLS 数据包传输层安全性协议(Datagram Transport Layer Security)

EEPROM 带电可擦可编程只读存储器(Electrically Erasable Programmable Read Only Memory)

ECC 椭圆加密算法（Elliptic curve cryptography）

IoT 物联网(Internet of Things)

LoRa 长距离无线电（Long Range）

LoRaWAN 长距离广域网（Long Range Wide Area Network）

MCU 微控制单元（Micro Controller Unit）

MF 主控文件(Master File)

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

NFC 近场通信（Near Field Communication）

OOB 带外传输（Out of Band）

PIN 个人识别码(Personal Identification Number)

RAM 随机存取存储器（Random Access Memory）

RSA 非对称加密算法(Rivest/Shamir/Adleman asymmetric algorithm)

SE 安全单元（Secure Element）

SHA-1 安全摘要算法1（Secure Hash Algorithm 1）

SM2 安全消息算法2（Secure Message 2）

SM4 安全消息算法4（Secure Message 4）

5 系统架构

智能门锁自动控制模块应包括主控模块、安全模块、按键模块、蓝牙开锁、读卡模块、通信模块、生物特征识别模块，也包含为电子模块提供软件能力的嵌入式系统，见图 1 所示，

并具备下列功能：

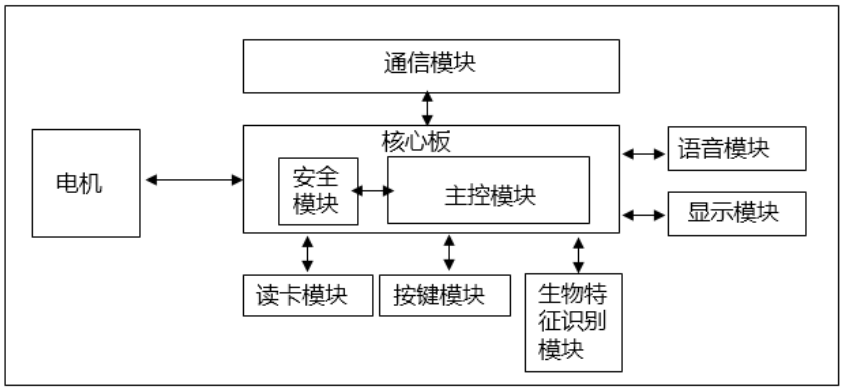

图1　智能门锁自动控制模块系统架构

a) 主控模块：实现智能门锁的用户界面、应用功能与逻辑控制等功能；
b) 安全模块：提供智能门锁的安全运算（如加解密运算、安全认证、数据校验、数据鉴权等）、敏感数据（如用户密码、用户 ID、卡片鉴权数据、关键代码、生物特征数据、设备根密钥等）的安全存储和电机控制等功能；
c) 按键模块：通过触控或者机械方式实现用户密码输入功能；
d) 蓝牙开锁：通过蓝牙连接方式实现开锁功能；
e) 读卡模块：实现智能卡开锁功能；
f) 通信模块:通过 BLE/zigbee/WAPI(Wi-Fi)/NB-IoT/LoRa/LoRaWAN/3G/4G/5G 等远、近场通信技术，实现门锁设备的网络接入，与云端进行连接通信等功能；
g) 生物特征识别模块:采集用户个体的生物特征信息,实现生物特征信息的比对功能。

6　主控模块

主控模块应符合下列要求：

a) 当 MCU 启动时，宜先与 SE 进行身份认证，认证通过后执行后续操作；
b) 当在 MCU 上需要保存密钥时，该密钥应该加密保存；
c) MCU 上的代码在更新前，应保证更新代码的真实性和完整性，只有合法的代码才能支持更新；
d) MCU 在判断是否转动电机开锁的变量时，应保证该变量的判断是复杂值，不是简单的 0 或者 1；
e) 在性能允许的情况下，在转动电机开锁前的鉴权认证应进行两次以上，以防止某次认证因为遭受注入攻击而被跳过；
f) 在关键的转动电机开锁的代码路径上应执行代码路径检查,以防止某些关键的路径因为遭受注入攻击而被跳过；
g) MCU 在检查到攻击的时候应该进行复位操作，复位后应保证转动电机使锁处在闭合状态；
h) MCU 应能够记录攻击或者开门鉴权错误的次数，当次数达到一定的阈值时，应该采取延时一段时间才能进行开门动作，随着攻击的次数越来越多延时应该越来越长，直到能够进行一次正确的开门鉴权为止；

i） 用户的敏感信息如白名单、黑名单和鉴权密钥等不应存放在 MCU 上，而应该存放在 SE 上。

7 安全模块

7.1 基本要求

安全模块应符合下列基本要求：

a） 支持真随机数发生，随机数应符合 GM/T 0005-2012 或 NIST SP800-22 的要求。
b） 支持常用对称密码算法，包含但不限于 SM4、DES、3DES；
c） 支持常用非对称密码算法，包含但不限于 SM2、RSA、ECC；
d） 支持常用杂凑算法，包含但不限于 SM3、SHA-1；
e） RSA 算法支持 1152 位及以上；
f） SM2 算法支持国密标准 256 位。

7.2 应用结构

安全模块主要包括访问控制、算法管理、用户管理、身份认证、安全支持和内存管理，具体结构见图 2。

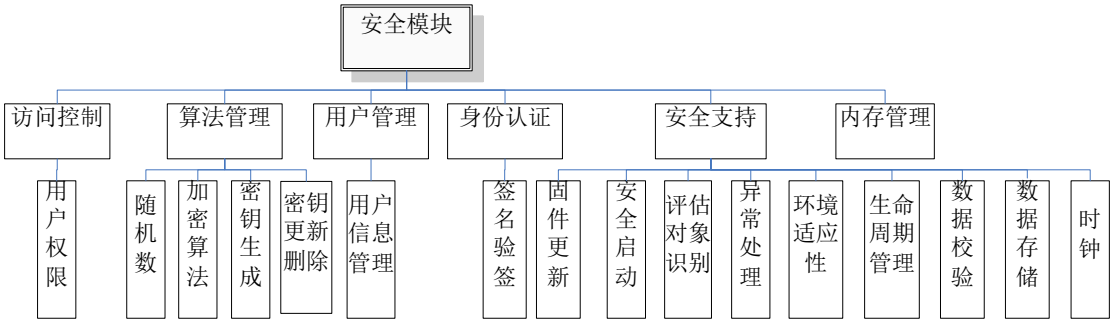

图2 安全模块应用结构

7.3 发行要求

安全模块应符合 GM/T 0008-2012 安全芯片密码检测准则；安全模块安全等级至少达到 GB/T 18336.3-2015 规定的评估保障级 2（EAL2）。

7.4 安全功能要求

7.4.1 安全模块识别

安全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。并符合以下要求：

a） 安全模块应支持与安全认证平台进行双向设备身份认证功能，安全模块与安全认证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） 安全模块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安全认证平台进行统一管理；
c） 安全模块身份识别信息应与门锁设备信息进行关联，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；

d) 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，使每个安全模块具有唯一的设备密钥，且设备根密钥与门锁终端身份识别信息绑定。门锁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。

7.4.2 异常处理

安全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，捕获异常后，应记录异常信息。

7.4.3 随机数

安全模块的随机数产生器应经过评估，确保其产生的随机数具有足够的随机性。随机数应符合GM/T 0005-2012或NIST SP800-22的要求。

7.4.4 访问权限控制

安全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。应具有用户使用权限管理功能，增加和删除用户前，应确保具备该操作权限。访问控制符合以下要求：

a) 应具有用户使用权限管理功能，在添加或删除用户的过程中，应具有相应的授权机制。同权限的账户应使用不同的密码和智能卡；
b) 当具有默认帐户时，应提示要求用户重命名或删除默认账户，修改默认账户的默认口令；
c) 应提供用户帐户删除功能，方便用户删除或停用账户；
d) 不应留有可访问程序区及数据区的调试接口。

7.4.5 安全启动

启动过程应是一个安全启动的过程。模块启动过程中检查到失败，模块及其功能应以安全的方式失效。

7.4.6 环境适应性

改变安全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）。

7.4.7 计时功能（可选）

模块应保证其时钟源的连续性与稳定性，确保计时准确。

7.4.8 密钥管理

7.4.8.1 密钥生成安全

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，发布版本的自动控制模块不应支持私钥的导出功能。模块产生的会话密钥，应保证每次会话的密钥不可预期。安全模块的会话密钥生成应满足：

a) 会话密钥应采用密钥派生算法得到，算法输入应包含主密钥、随机数；
b) 每次会话应生成不同的随机数以获得不同的会话密钥；
c) 通信应采用会话密钥加密以保证通信的机密性；
d) 通信数据应进行完整性校验以保证消息不被篡改。

7.4.8.2 密钥更新和删除

安全模块管理密钥更新和删除时，应验证具备该操作权限，且更新密钥时，密钥长度应满足要求，非对称密钥应满足是素数。

7.4.8.3 内存管理单元

当安全模块预期支持多应用环境时，安全模块应具有内存管理单元，保证不同应用之间数据隔离。

7.4.8.4 敏感数据管理

安全模块应管理开锁过程中的敏感数据（PIN、蓝牙用户信息、生物特征等信息）的存储、校验和修改，并满足如下要求：

a) 模块内存储的敏感数据应有加密存储和使用时进行完整性校验；
b) 加密敏感数据使用的密钥，应满足每一个模块都不相同，即一机一密的要求；
c) 加密敏感数据使用的算法强度应不低于 AES-128，完整性校验使用的算法强度应不低于 CRC32。

7.4.8.5 签名验签

应提供身份认证的签名和验签算法，为身份认证提供算法支撑。

7.4.8.6 身份认证

应提供身份认证算法，保证通信双方是经过身份认证的。

7.4.8.7 固件更新

当智能门锁固件能够进行更新（脱机或者在线）时，智能门锁应验证更新固件的完整性和真实性。固件镜像中应植入验证固件的公钥。只有经过认证且由固件开发者提供的固件镜像才允许更新。当固件的完整性和真实性校验失败时，智能门锁应拒绝进行固件更新。并符合下列要求：

a) 固件更新首先应进行认证操作，以确认更新源的合法性；
b) 应拒绝旧版本固件的回滚更新，厂家可自定义能够更新的固件版本范围。

7.4.8.8 生命周期管理

应提供生命周期管理，保护开发、测试和使用和销毁各阶段关键资产的安全。

7.4.8.9 数据存储

应提供敏感数据（如用户密码、用户ID、PIN、卡片鉴权数据、关键代码、生物特征数据、设备根密钥等）的安全存储功能，保证数据的完整性和机密性，防止泄露敏感数据。

7.4.8.10 数据校验

应提供用户密码、用户ID、卡片鉴权数据、生物特征数据的校验功能，校验过程应防止泄露数据。

7.5 抗攻击能力要求

7.5.1 物理防护

应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。

7.5.2 测试模式激活

应具有足够的防护措施保证模块不易返回特权模式（如芯片测试模式和开发模式）导致敏感信息的泄露。当安全模块注入工作密钥后，则不能再进入测试态。

7.5.3 侧信道分析

应具备足够的防护，防止攻击者通过 SPA、DPA、EMA 即可获取存储于模块内的密钥或者其他敏感数据。

7.5.4 故障注入

应具备足够的防护，防止攻击者利用故障注入手段，如毛刺、强电场、强磁场等，干扰模块加解密过程，导致密钥信息泄露。

7.5.5 环境压力攻击

应具备防护环境压力（如高低电压、高低温度和高低时钟）攻击的能力，防止攻击者干扰模块正常工作，导致敏感信息泄露（如认证密钥或 PIN 等）或跳过关键操作（如跳过 PIN 校验直接开锁）。

7.5.6 恶意代码攻击

应具备防护恶意修改攻击（例如植入木马、后门等）的能力，防止攻击者获取用户敏感信息，或者控制设备。

7.6 文件结构

7.6.1 一般规定

安全模块的密钥数据、敏感数据以及应用数据的储存，宜采用文件的方式来管理，并应至少提供密钥文件、发行文件以及应用密钥文件。

7.6.2 密钥文件

安全模块中的密钥文件应符合表 1 的要求。

表1 安全模块密钥文件

密钥名称	密钥代码	密钥标识	密钥分散级别	密钥作用
主控密钥	SECK	0	3	控制MF下文件添加和删除；
维护密钥	SEMK	0	3	MF下文件的更新保护
认证密钥	—	0	3	用于认证激活使用

7.6.3 发行文件

安全模块中的发行文件应符合表 2 的要求。

表2　安全模块发行文件

文件标识符	‘0015’	
文件类型	线路保护的二进制文件	
文件主体空间	‘1E’	
读权限	自由读取	
写权限	写二进制时必须使用 SEMK 进行线路保护，如连续三次执行此命令失败，SE 回送‘9303’即应用永久锁定	
字节	数据元	长度
1-8	SE 发行方标识	8
9	应用类型标识	1
10	应用版本	1
11-12	占位符（0000）	2
13-20	应用序列号	8
21-24	应用启动日期	4
25-28	应用有效日期	4
29-30	SE 发行方自定义文件控制信息数据	2

7.6.4　应用密钥文件

安全模块中的应用密钥文件应符合表3的要求。

表3　安全模块应用密钥文件

分类	名称	说明	密钥分散和存储			功能
			行业	运营商	卡商	
ADF 身份识别应用	DACK	应用主控密钥	项目编号 芯片ID	—	—	应用认证激活
	DAMK	应用维护密钥	项目编号 芯片ID	—	—	应用文件修改
	—	应用安全传输密钥	项目编号 芯片ID	项目编号	—	芯片安全通讯保护（密文+MAC）
	DPUK	PIN解锁密钥	项目编号 芯片ID	项目编号	—	口令识别
	DPRK	PIN重装密钥	项目编号 芯片ID	项目编号	—	口令识别
	DENCK	认证密钥	项目编号		IC卡： 项目编号	开锁密钥

					卡号	
	—	应用预留	项目编号	—	—	—
	—	应用预留	项目编号	—	—	—

安全模块中的公钥文件应符合表4的要求。

表4　安全模块公钥文件

文件标识符	‘0128’
文件类型	线路保护的二进制文件
文件主体空间	—
读权限	无条件
写权限	线路保护

7.7　认证激活

安全模块认证激活流程见图3。

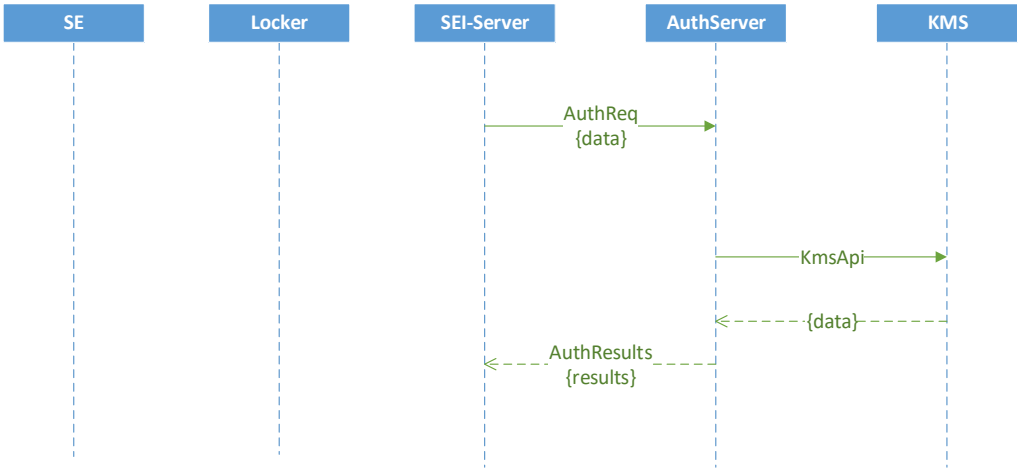

图3　安全模块认证激活流程

8　按键模块

8.1　安全要求

按键模块应满足下列要求：

a）　应提供防偷窥机制或虚位密码功能，以保护用户的PIN信息；

b）　当配装显示屏时，在密码按键上输入的PIN应以无意义字符显示；

c）　在输入PIN时按键提示音或机械音应保证一致，不应泄露敏感数据或者足够随机不会泄露敏感信息；

d）　当带有震动反馈或能引起震动时，应保证所有按键引起的震动保持一致，无差异或者足够随机不会泄露敏感信息；

e）　应考虑在输入PIN后，键盘按键上无明显的热残留信息；

f） 应支持的最大密码长度不低于6位；

g） 应设置安全密码逻辑，防止暴力破解和穷举PIN；

h） 应急充电接口应只能用于补电，不存在逻辑异常及后门开锁指令；

i） 在输入PIN并完成校验后，应及时清除PIN信息，防止内存中残留PIN信息。

8.2 开锁流程

通过按键方式的开锁流程见图4。

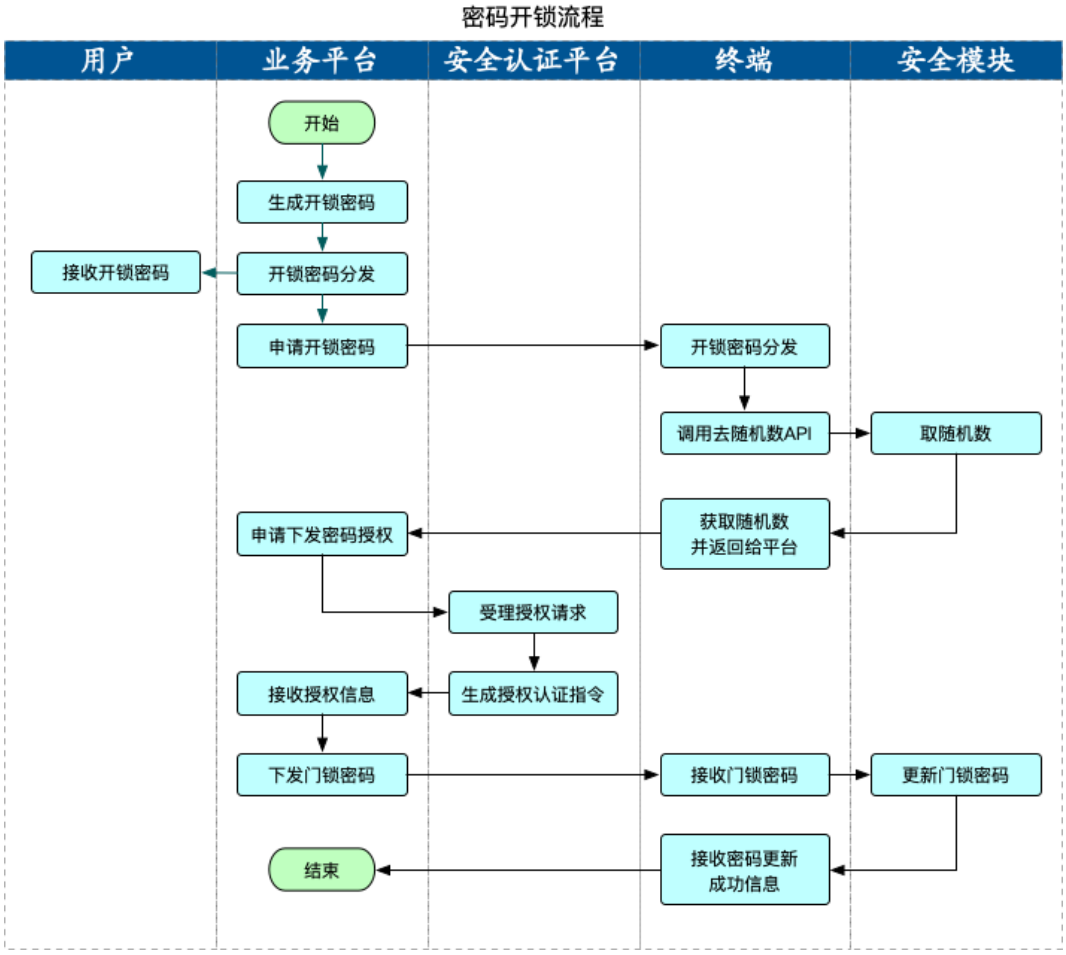

图4 密码开锁流程

8.3 验证密码

验证密码（Verify PIN）流程应符合表5的要求。

表5 验证密码流程

外部	终端	SE
请求开锁 调用 Verify PIN SDK =>		
	发送 Verify PIN 命令 =>	
		<= 响应 Verify PIN 命令
	判断是否 9000 如是 9000 返回 true；	

	如不是 9000 返回 false <= 返回 PIN 校验状态	
接收结果判断，是否开锁		

8.4 修改密码

修改密码（Change PIN）流程应符合表6的要求。

表6 修改密码流程

外部	终端	SE
请求修改 PIN 调用 Change PIN SDK =>		
	发送 Change PIN 命令 =>	
		<= 响应 Change PIN 命令
	判断是否 9000 如是 9000 返回 true； 如不是 9000 返回 false <= 返回 Change PIN 结果	
接收结果判断 修改 PIN 是否成功		

8.5 重置密码

重置密码（Reload PIN）流程应符合表7的要求。

表7 重置密码流程

外部	终端	SE
收到取随机数请求 调用 Get Random SDK =>		
	发送 Get Random 命令 =>	
		<= 响应 Get Random 命令
	<= 返回随机数	
使用随机数向安全认证平台 请求命令 MAC		
收到 MAC 后打包命令， 调用 Direct Send SDK =>		
	发送命令 =>	
		<= 返回结果

9 蓝牙模块

9.1 基本要求

蓝牙模块开锁的基本要求应包括：

a) 当使用低功耗蓝牙（BLE）进行设备入网时，应采用PassKey Entry、Numeric Comparison、OOB模式授权配网，或者当采用Just Work方式匹配时，应有效防止中间人攻击；

b) 通信模块与钥匙载体或者网关之间的通信数据，应支持国密算法加密传输，且可选支持国际算法；

c) 安全传输协议应支持DTLS；

d) 应支持软件认证加密能力,宜支持专用硬件认证加密模块，应至少支持国密算法，且可选支持国际算法；

e) 当使用远程密钥下发技术，应支持发送方与接受方之间的双向认证，防止敏感数据被泄露或篡改，“会话密钥”并应保证一次一密。

9.2 开锁流程

蓝牙模块开锁流程见图5。

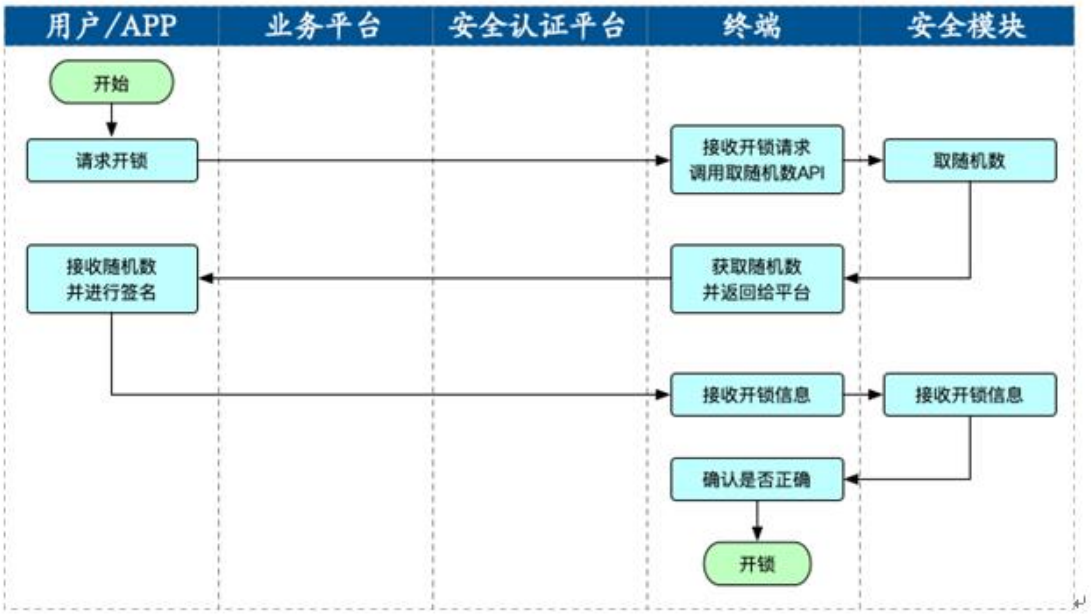

图5 蓝牙模块开锁流程

9.3 认证流程

蓝牙模块认证流程见图6。

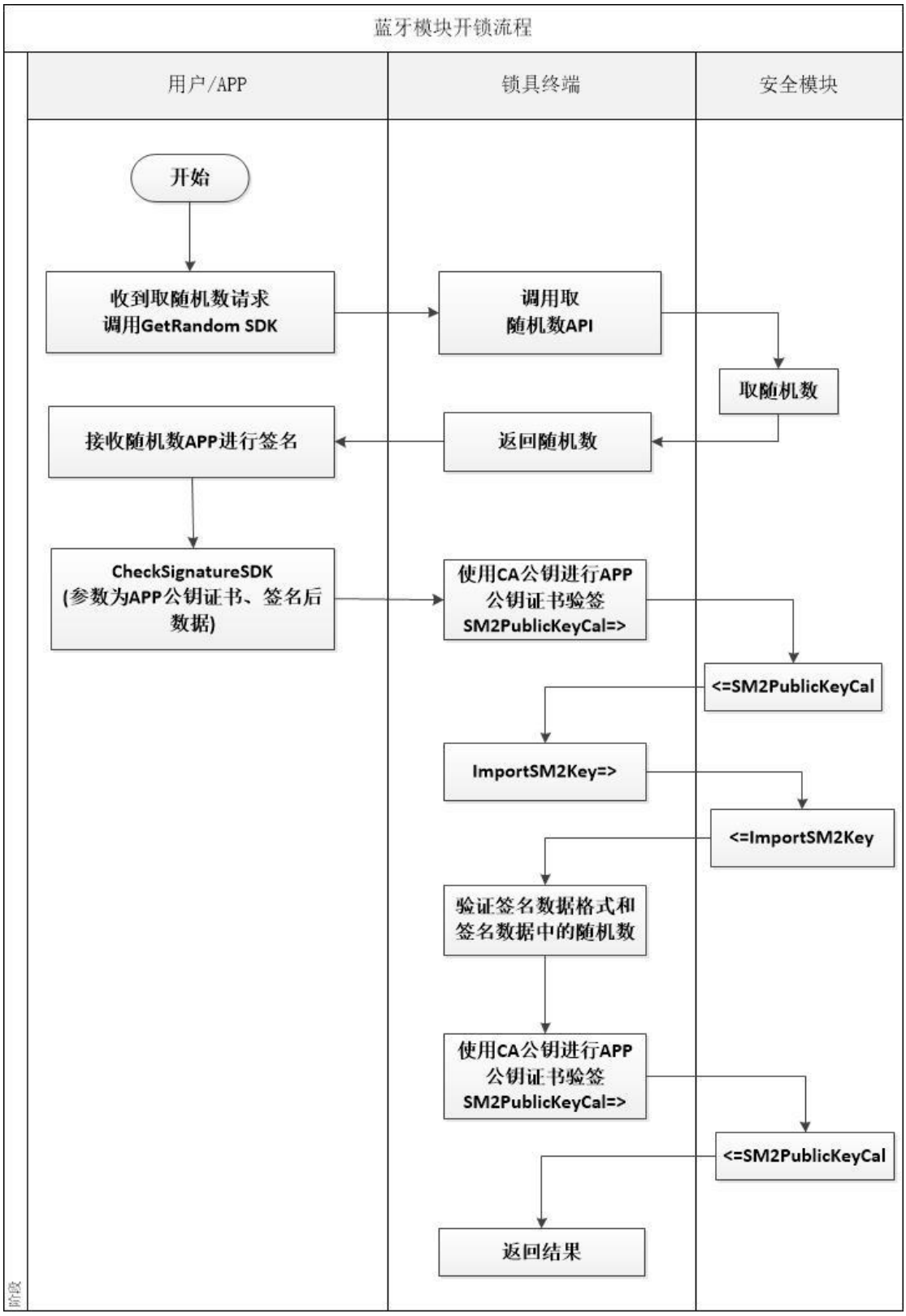
蓝牙模块开锁流程
用户/APP
锁具终端
安全模块
开始
收到取随机数请求
调用GetRandom SDK
调用取
随机数API
取随机数
接收随机数APP进行签名
返回随机数
CheckSignatureSDK
(参数为APP公钥证书、签名后
数据)
使用CA公钥进行APP
公钥证书验签
SM2PublicKeyCal=>
<=SM2PublicKeyCal
ImportSM2Key=>
<=ImportSM2Key
验证签名数据格式和
签名数据中的随机数
使用CA公钥进行APP
公钥证书验签
SM2PublicKeyCal=>
<=SM2PublicKeyCal
返回结果

图6　蓝牙模块认证流程

10　读卡模块

10.1　基本要求

读卡模块应符合下列要求：

a)　符合 ISO/IEC 14443 Type A/B 协议；

b)　应具有低功耗寻卡功能；

c)　读卡模块和主控模块的通信接口应支持但不限于 I2C 或 SPI；

d)　输出射频场强应不小于 1.5A/m；

e)　支持读取身份证时，应符合 GA 450-2013 和 GA 1153-2014 的要求。

10.2　应用流程

10.2.1　绑定流程

智能门锁与卡片的绑定流程见图7。

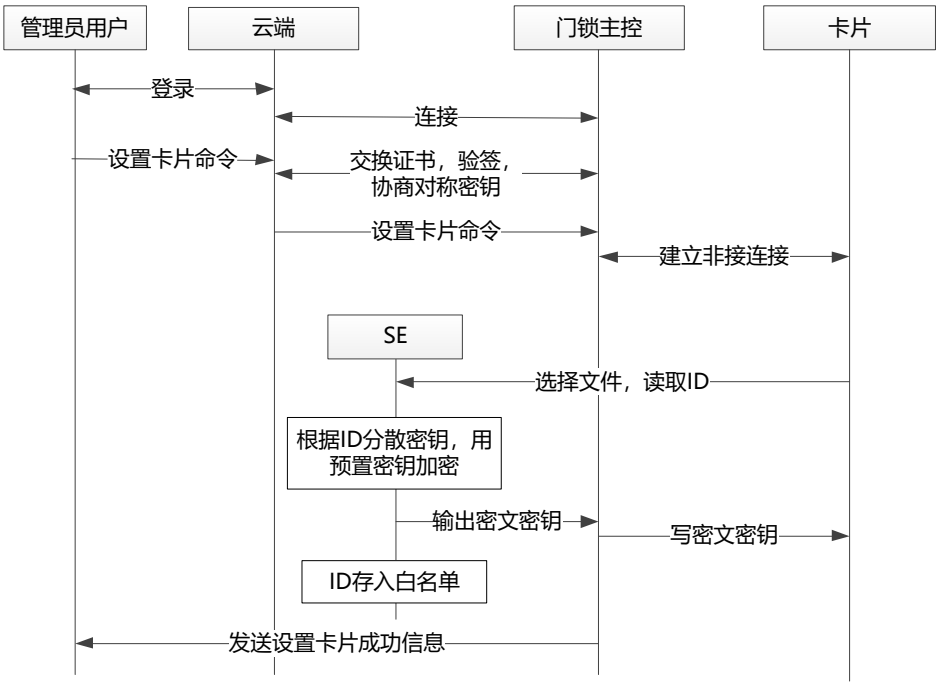

图7　智能门锁与卡片绑定流程

10.2.2　识别流程

智能门锁与卡片的识别流程见图8。

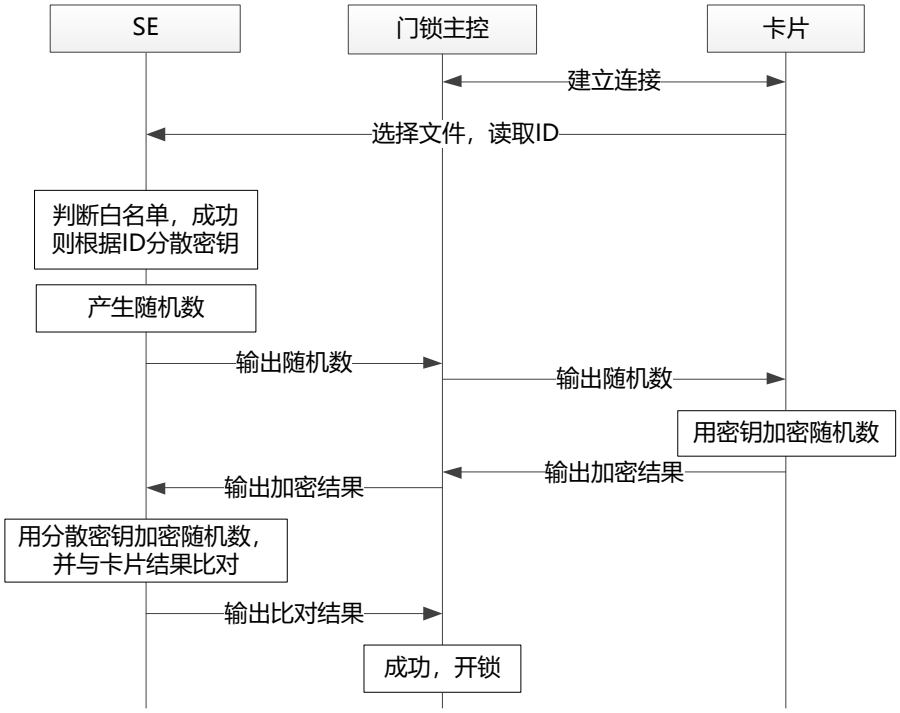

图8　智能门锁与卡片识别流程

10.2.3　解绑流程

智能门锁与卡片的解绑流程见图9。

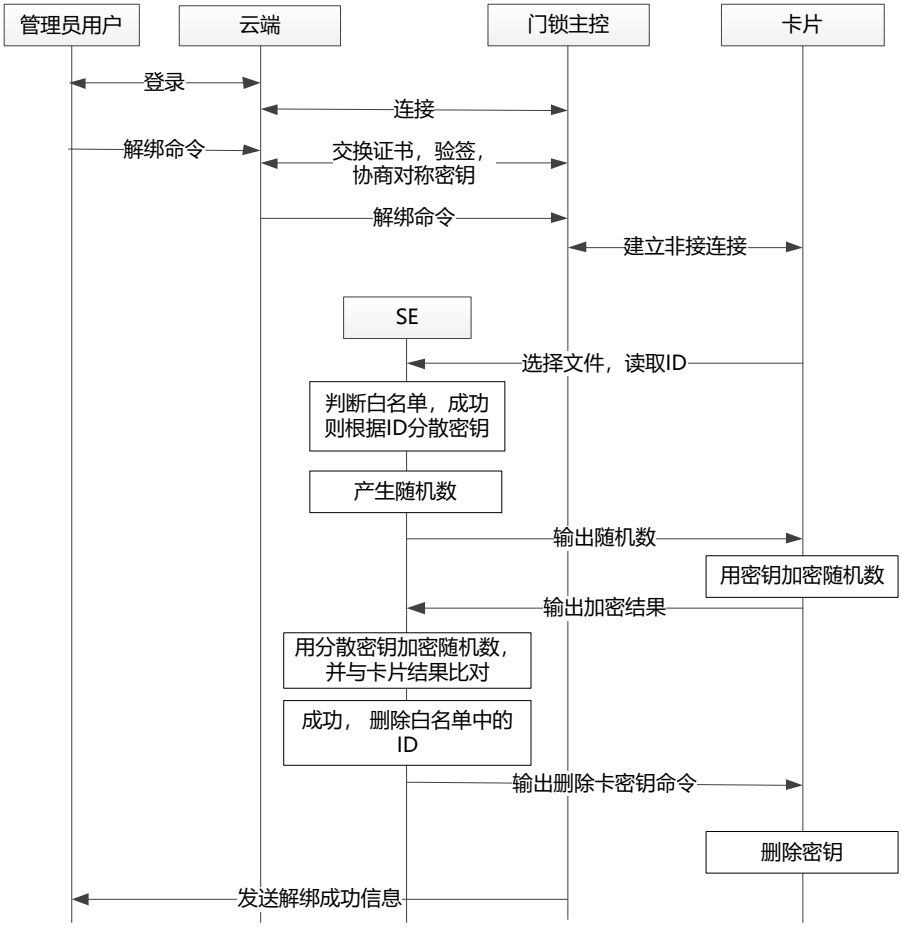

图9　智能门锁与卡片解绑流程

11　通信模块

11.1　基本要求

通信模块应符合下列基本要求：

a)　通信模块应支持一种或多种通信技术（例如，LoRa，NB-IoT，2G/3G/4G/5G）；

b)　采用 LoRa 通信模块时，宜采用 ClassB 实时性增强以及网关同步等方案，以提升网络时效性；

c)　联网传输协议应支持国内外主流协议的一种或多种（如 HTTP 协议，MQTT 协议等）；

d)　通信数据传输的时效性、准确率应符合联网技术要求。

11.2　设备入网安全

当采用标准通信协议（如蓝牙、zigbee，NB-IoT等）进行设备的入网许可时，应符合下列要求：

a)　当使用低功耗蓝牙（BLE）进行设备入网时，应采用 PassKey Entry、Numeric Comparison、OOB 模式授权配网，或者当采用 Just Work 方式匹配时，应有效防止中间人攻击；

b) 当使用 zigbee 技术进行设备入网时，应采用 zigbee3.0 Install Code/PreInstall Key 的安全模式授权匹配，或者当采用非 zigbee3.0 Install Code/PreInstall Key 的模式配网时，应有效防止中间人攻击；
c) 当使用 WAPI（Wi-Fi）技术进行设备入网时，应采用 WPA2 及以上版本协议；
d) 当使用 NB-IoT 无线通信加密和鉴权要求时，NB-IoT 通信的鉴权、加密和完整性保护应符合相关标准的要求；
e) 当使用 LoRa 无线通信加密和鉴权要求时，LoRa 通信的鉴权，加密和完整性保护应符合相关标准的要求。

11.3 数据传输安全

智能锁以无线方式开锁或者进行密钥下发等敏感数据交互时，通信双方应进行认证，防止敏感数据被泄露或篡改，并应符合下列要求：

a) 采用蓝牙、WAPI（Wi-Fi）、zigbee 等技术，通信模块与钥匙载体或者网关之间的通信要求应符合国家密码管理关于算法的要求；
b) 采用 NB-IoT 或 LoRa 通信模块与云服务平台间认证加密时，应符合下列要求：
   1) 安全传输协议：应支持 DTLS；
   2) 认证加密能力：应支持软件认证加密能力,宜支持专用硬件认证加密模块。

11.4 认证加密能力

具有数据存储和设备管理的通信设备，应使用硬件安全模块进行加密计算。

12 生物特征识别模块

12.1 指纹开锁

12.1.1 通用技术要求

指纹身份识别模块通用技术应包括登记、识别和注销三个过程。

12.1.2 基本功能和性能要求

指纹识别模块应包括但不限于如下功能和要求：

——应支持用户已登记指纹更新、新增指纹、已登记用户指纹注销功能；

——应支持用户使用指纹识别模块实现用户指纹识别功能；

——指纹识别模块应支持指纹360度可识别；

——门锁管理APP或外部设备应具有明确的用户提示，告知用户对其指纹样本进行了采集；

——应能对登记的用户指纹样本进行质量判断，以确定当前指纹特征样本是否满足指纹特征识别处理的需求。宜支持对指纹样本质量指标进行设定。指纹特征样本未通过质量判断时应具备相应的处理机制，如提示用户重新采集或提示失败等；

——在指纹身份识别模块上登记的用户指纹，在存储和传输过程中应遵循 GB/T 26237 所规定的指纹特征数据交换格式，将事件的标识符、唯一的设备标识符、登记日期和时间等数据作为指纹特征数据的扩展项一同执行；

——应具备异常情况处理能力，包括但不限于指纹采集失败、指纹登记失败、指纹删除失败、指纹比对失败后的处理机制；

——指纹身份识别模块上可登记指纹数量不小于2个；

——基于良好的供电环境下，指纹身份识别模块完成单次指纹数据信息采集并完成录入的总时间（从用户手指接触到指纹传感器开始到输出录入结果为止的时间跨度）应小于等于3000ms；

——基于良好的供电环境下，指纹身份识别模块完成指纹数据信息采集并完成识别的总时间（从用户手指接触到指纹传感器开始到输出识别结果为止的时间跨度）宜小于等于2000ms（基于2个指纹模板）；

——指纹识别的准确性应至少满足如下指标：基于 1:1 比对，当错误接受率(False Acceptance Rate)为 1/10000 时，错误拒绝率（False Rejection Rate）不高于3%。

12.1.3 逻辑接口与命令要求

逻辑接口命令用于指纹模块的指纹注册、指纹验证的外部调用。主要包括如下四个接口：

——指纹注册接口命令；

——指纹验证命令；

——指纹更新命令；

——指纹注销命令。

12.1.4 信息安全要求

12.1.4.1 基础安全要求

在基础安全要求方面，应满足如下要求：

——指纹处理单元应具备数据保护功能和抵抗错误注入、侧信道攻击的能力，应保证指纹信息不被提取、窃取；

——在指纹特征的采集、传输、存储和比对过程中，需具备必要的保护机制，用于保护指纹特征数据的安全；

——在指纹模板比对后，比对结果的传输过程应进行加密或使用私钥签名保护，确保通过各个接口输出的对比结果（IIC、UART、USB等）不被篡改；传输环境应具备抵抗重放攻击、错误注入攻击、随机数发生器攻击的能力；以及针对以上保护机制中所涉及的密钥的错误注入、侧信道攻击。

12.1.4.2 指纹采集安全要求

指纹采集应符合下列安全要求：

——采集过程应在独立的逻辑域或物理域中实现；

——应具备有效的安全机制，确保指纹特征样本采集、质量判断、呈现攻击检测(若有)、指纹特征项提取和传输过程中的用户指纹特征数据的机密性和完整性；

——应及时清除未通过质量判断的用户指纹特征样本，并确保其不可恢复；

——指纹特征项提取结束后应及时清除用户的指纹特征样本，并确保其不可恢复；

——指纹采集模块除与主控芯片有接口外，不得在模块外设有额外通信接口；

——指纹采集模块应使用无算力的传感器及其配套元器件，不应具备存留指纹等敏感信息的能力，不应具备影响指纹处理单元（MCU）、安全模块（SE）安全工作的能力。

12.1.4.3 指纹存储安全要求

指纹存储应符合下列安全要求：

——应具备有效的安全机制，防止对指纹存储区的非授权访问、恶意篡改；

——具有有效的安全机制，确保已注册用户指纹特征模板与该用户标识之间的正确关联关系，防止被非法修改；

——应具备有效的安全机制，确保在对指纹存储区中用户指纹特征数据进行操作时，如存储和传输时，用户指纹特征数据的机密性和完整性，并在操作完成后对操作过程中的临时数据（如存储或传输过程中，留存在设备动态内存中的与指纹特征样本等数据），进行及时清除并确保不可恢复；

——宜采用加密方式对用户指纹特征模板数据进行存储；

——对于已删除的用户指纹特征模板数据，应及时进行清除并确保不可恢复。

12.1.4.4 指纹比对安全要求

指纹比对应符合下列安全要求：

——比对过程应在独立的逻辑域或物理域（例如SE、MCU）中实现；

——应具备有效的安全机制，确保在进行指纹特征比对操作时：

- 指纹特征模板读取的准确性；
- 指纹特征数据不被窃取或篡改；
- 相似度计算结果不被窃取或篡改；
- 识别决策结果不被窃取或篡改；
- 比对结束后，应及时清除持卡人指纹特征数据和比对过程中所产生的其他临时数据（如比对得分等）。

——每次对比，不论指纹特征样本与指纹特征模板相似度如何，对比过程均有相似的耗时与耗能，以防范攻击者通过相关信息的分析来猜测指纹特征模板的数据；

——应设定比对失败尝试次数限制，比对失败次数超出限制后，应采取相应的失败处理机制；

——应采取有效的安全机制，确保识别结果输出时的完整性，不被非法篡改。

12.2 人脸识别开锁

12.2.1 通用流程要求

人脸识别模块通用技术包括人脸注册、人脸识别、人脸变更和人脸注销。

12.2.2 基本功能要求

12.2.2.1 人脸注册

人脸注册包括人脸数据的采集、传输、存储和用户身份的绑定等功能，应满足以下要求：

——对用户身份进行认证，应采用多因素确保用户身份的真实性；

——取得用户的明示同意；

——对人脸采集对象进行活体检测，保证采集到的人脸样本来自活体。

12.2.2.2 人脸识别

人脸识别包括质量判断、特征提取、特征比对及决策等功能，应满足以下要求：

——宜对人脸采集对象进行活体检测；

——采用脱机方式，人脸识别模块应进行人脸识别的特征提取、特征比对；

——采用联机方式，人脸路由网关应进行人脸识别的特征提取、特征比对。

12.2.2.3 人脸变更

人脸变更是指重新采集人脸样本以实现对原有人脸模板的更新，根据发起方不同分为样本后台/门锁主动发起和用户主动发起两种，应满足以下要求：

——对用户身份进行认证，应采用多因素确保用户身份的真实性；

——应对人脸采集对象进行活体检测，保证重新采集到的人脸样本来自活体；

——取得用户的明示同意；

——保证人脸信息同步。

12.2.2.4 人脸注销

人脸注销包括将用户人脸数据样本后台/本地人脸特征存储模块中删除，并解除与用户的关联关系等功能，应满足以下要求：

——对用户身份进行认证，确保用户身份的真实性；

——取得用户的明示同意；

——保证人脸信息同步。

12.2.3 性能要求

12.2.3.1 活体检测性能

活体检测应能防范的二维假体攻击包括但不限于二维静态纸质图像攻击、二维静态电子图像攻击、二维动态图像攻击等。

活体检测应能防范的三维假体攻击包括但不限于三维面具攻击、三维头模攻击等。

活体检测性能要求分为基本级和增强级，防范二维和三维假体攻击次数比例为 9:1 时，性能指标要求应符合表 8 的要求。

表8 活体检测性能指标要求

分级	防范假体攻击
基本级	当LDAFAR为1%时，LPFRR≤1%
增强级	当LDAFAR为0.1%时，LPFRR≤1%

12.2.3.2 人脸辨识性能

人脸辨识性能指标应符合表9的要求。

表9 人脸辨识性能指标要求

人脸库数量	人脸辨识性能指标
N=500	当误识率为万分之一时，通过率≥ 98.3% 当误识率为十万分之一时，通过率≥ 98%

12.2.4 质量判断要求

12.2.4.1 评估要求

2D人脸数据样本后台/本地人脸特征存储模块应对用于人脸识别的数据质量进行评估，包括但不限于：

——人脸区域大小评估，判断检测到的人脸区域大小是否符合人脸识别算法要求；

——清晰度评估，判断人脸区域是否清晰；

——完整度评估，判断人脸区域是否完整；

——表情评估，判断人脸表情是否合理；

——姿态角度评估,判断人脸姿态的旋转角度、俯仰角度和倾斜角度是否在合理范围内；
——眼睛闭合程度评估，对眼睛的闭合程度进行评估并判断是否合理；
——嘴巴闭合程度评估，对嘴巴的闭合程度进行评估并判断是否合理；
——光照度评估，判断人脸区域的光照是否合理。

3D 人脸数据样本的人脸识别数据质量评估要求，包含但不限于：
——数据完整性要求：拥有完整的 RGB 图像、IR 图像、深度图像，且三路图像所拍场景需要基本重合；深度图像完整率占比>80%；
——距离要求：在 30cm-120cm 范围内的图像需要满足人脸识别、活体检测算法的数据精度要求；
——对齐要求：RGB、深度图像之间的像素点需要有固定的映射关系，且算法端可以获取这种映射关系，并满足算法的精度要求。

12.2.4.2 质量要求

人脸处理模块应按照如下质量要求选取人脸数据用于人脸辨识：
——人脸全景图分辨率应不低于 640*480 像素；
——人脸全景图应能准确确定人脸识别对象；
——人脸大小应满足以下要求：
- 对于注册人脸图像，瞳间距应不小于60像素，宜大于90像素；
- 对于识别人脸图像，瞳间距应不小于60像素，宜大于90像素。

——人脸区域应清晰，人脸图像的清晰度应满足以下要求：
- 对于注册人脸图像，运动模糊小于等于0.15，高斯模糊小于等于0.24；
- 对于识别人脸图像，运动模糊小于等于0.20，高斯模糊小于等于0.25。

——人脸区域需要完整,轮廓和五官清晰,无浓妆,图像脸部区域应无编辑修改性处理，几何失真应小于等于 10%，眼镜框应不遮挡眼睛，镜片无色无反光。人脸图像的完整度应满足以下要求：
- 对于注册人脸图像，几何失真应小于等于5%；
- 对于识别人脸图像，几何失真应小于等于10%。

——人脸图像的表情应合理，中性或微笑，眼睛自然睁开，嘴唇自然闭合或微张；
——人脸姿态需要在合理范围内，应满足以下要求：
- 注册人脸图像旋转角应在±20°以内，俯仰角应在±20°以内，倾斜角应在±20°以内；
- 识别人脸图像旋转角应在±20°以内，俯仰角应在±20°以内，倾斜角应在±20°以内。

——人脸区域光照均匀，对比度适中，脸部无明显阴影、无过曝光和无欠曝光，图像灰度化后脸部区域动态范围主要分布在 85~200 间，灰度级应为 256 级；
——人脸区域深度图数据完整性大于 80%，精度小于 5mm@1m。

12.3 声纹开锁

12.3.1 通用技术要求

12.3.1.1 声纹注册

声纹的注册功能应包括语音信息的采集、传输、声纹模型的建立、声纹特征存储和用户身份的绑定等。声纹的注册应满足以下要求：

a） 注册前需对用户身份进行认证；

b） 注册前应取得用户的明示同意；

c） 声纹传输时应包含用户属性数据，如用户唯一性标识、移动设备标识等；

d） 声纹存储时应与用户属性数据形成映射关系。

12.3.1.2 声纹验证

声纹的验证功能应包含对满足语音质量要求的待验证语音提取声纹特征，进行声纹特征确认等，实现关联账户的主体身份的验证。

用于开锁凭证的动态声纹密码应由服务器端生成，并应满足以下要求：

a） 不低于 6 位；

b） 有效期不超过 5 分钟；

c） 避免连续重复，如“…11…”等；

d） 验证后应及时清除。

12.3.1.3 声纹变更

声纹的变更功能应包含对采集到的语音信息传输至服务器端，服务器端重新对原有的声纹模型进行训练以实现对原有声纹信息的更新。应符合下列要求：

a） 声纹的变更在发起方上分为系统主动发起、声纹信息控制者主动发起和用户主动发起；

b） 系统主动发起的变更为系统初始设计时定义的内部模型更新；

c） 声纹信息控制者主动发起的变更为因业务、技术因素等需变更算法或模型架构涉及的调整，如算法厂商变更、算法/模型重设计等；

d） 用户主动发起的变更为由用户主动意愿发起的自有声纹模型的变更，并应满足以下要求：

1） 变更前应对用户身份进行认证；

2） 变更前应取得用户的明示同意。

12.3.1.4 声纹注销

声纹的注销功能，由声纹信息控制者主动发起的和用户主动发起的对声纹功能的注销。声纹信息控制者主动发起对声纹的注销功能时，应满足以下要求：

a） 明确告知用户注销原因；

b） 明确告知用户注销时间。

用户主动发起对声纹的注销功能应满足以下要求：

a） 注销前应对用户身份进行认证；

b） 注销前应取得用户的明示同意；

c） 注销后应删除与用户相关的声纹信息或做匿名化处理，不可重复使用。

12.3.2 性能要求

12.3.2.1 基本性能指标

基本性能指标应同时满足错误接受率(FAR)≤0.5%、错误拒绝率(FRR)≤3.0%。

12.3.2.2 语音信息质量判断

应具备语音信息质量判断的能力，质量判断应包括但不限于截幅比例、信噪比、完整程度。

12.3.2.3 采样指标

采样指标应满足以下要求：

a) 采样率：16kHz；
b) 采样精度：16bit；
c) 声纹的注册时，有效语音长度≥5000ms；
d) 声纹的验证时，有效语音长度≥1000ms。

12.3.2.4 时间指标

时间指标应满足以下要求：

a) 声纹的注册时，系统响应时间：≤3000ms；
b) 声纹的验证时，系统响应时间：≤2000ms。

12.3.2.5 抗噪音能力

应具有一定程度的抗噪音能力，以保证系统的可用性。

12.3.2.6 抗时变能力

应具有因时间变化而导致声音变化的正确处理能力，以保证系统的可用性。

12.3.3 安全要求

12.3.3.1 声纹信息的采集

12.3.3.1.1 采集身份认证

声纹注册采集语音信息前，采用多种要素验证用户身份，应采用以下方式之一：

a) 采用符合《金融电子认证规范》（JR/T 0118）的数字证书，并组合登录密码等至少一种认证要素；
b) 采用符合 GB/T 38556-2020 要求的动态令牌设备，并组合登录密码等至少一种认证要素；
c) 至少组合两种认证要素（其中至少一种为动态认证要素，如动态验证码、基于客户行为的动态挑战应答等），并采用短信、数据（如即时通讯、邮件）等至少两种不同通信渠道。

12.3.3.1.2 明示同意

应向被采集用户进行必要明示，并明确告知声纹信息收集、使用信息的目的、方式和范围，征得用户同意后方可进行采集。

12.3.3.1.3 采集要求

声纹信息采集应符合下列要求：

a) 声纹信息的采集应使用动态声纹密码；
b) 声纹采集完成后，应立即对声纹信息进行加密处理；
c) 在声纹的注册时，声纹信息的采集宜使用多组动态声纹密码；
d) 采取安全措施保证声纹信息不被其他设备或程序非授权获取；
e) 采取防篡改机制保证声纹信息不被其他设备或程序篡改。

12.3.3.2 声纹信息的传输

应采用安全传输协议，保证声纹信息传输时的完整性和保密性。

应禁止向其他客户端应用软件提供声纹信息。

声纹识别接口不应暴露在公共、开放的网络上，应仅限于服务器端之间内部调用。

采集和产生的声纹信息应当在境内存储。因业务需要，确需向境外提供的，应符合相关的法律法规要求。

12.3.3.3 声纹信息的存储

12.3.3.3.1 客户端存储要求

门锁应用应禁止以任何形式留存声纹信息，包含声纹采集、声纹验证等过程中使用的声纹信息等。

12.3.3.3.2 存储措施

服务器端应加密保存声纹模型，并防止声纹模型的未授权访问、泄露、篡改或者毁损。

服务器端如留存语音信息，应对语音信息进行加密或采取高强度安全防护措施防止语音信息的未授权访问、泄露、篡改或者毁损；应对语音信息去标识化或脱敏处理，以确保对外不可用。

在发生或者可能发生声纹信息遗失、泄露或者毁损等情况时，应当立即采取补救措施，及时告知用户。

12.3.3.3.3 存储时间

服务器端留存的声纹模型信息保存时间应为实现目的所必需的最短时间。

12.3.3.4 声纹信息处理

12.3.3.4.1 用途

声纹信息不应转让，禁止用于声纹注册、验证、变更、注销之外的其他用途，但是法律另有规定的除外。

12.3.3.4.2 配置保护

声纹的验证应具有失败处理措施，在失败时应作出相应提示并进行失败次数限制，如果超过限制次数，则应触发相应的失败控制机制。

应采取有效措施，防止声纹模型配置参数的未授权访问、泄露、篡改等。

12.3.3.4.3 日志记录

在声纹的注册、验证、变更和注销环节，应对关键操作信息进行日志记录

12.3.3.4.4 处理身份认证

用户主动发起声纹变更、注销前，应采用12.4.1.1中要求的身份认证方式验证用户身份

12.3.3.4.5 防攻击能力

应具备抵御常见攻击的能力，包括但不限于：

a) 防语音模仿：在声纹确认过程中，应能够抵御攻击者通过模仿说话人，试图以说话人的身份通过声纹验证的攻击行为；
b) 防语音转换及合成：在声纹确认过程中，应能够抵御攻击者通过机械的、电子的方法产生人造语音的攻击行为，如语音合成技术；
c) 防录音欺诈:在声纹确认过程中，应能够抵御通过播放已经录制好的目标用户的声音尝试通过声纹验证的攻击行为；
d) 防录音拼接欺诈:在声纹确认过程中，应能够抵御把已经录制好的目标用户录音片段通过软件拼接成待验证语音，然后播放尝试通过声纹验证的攻击行为。

12.3.3.5 声纹信息删除

声纹信息删除后，应确保不可被检索、访问。