TC260-PG-2026NA

网络安全标准实践指南

——网络安全标识 消费类智能门锁安全要求

（征求意见稿 v1.0-202611）

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会秘书处

2026 年 11 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：

本文件主要起草人：

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

摘　要

伴随着消费类智能门锁的广泛应用，相关安全问题引发社会和业界高度关注。为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，全国网络安全标准化技术委员会秘书处组织制定了本文件，从物理与硬件安全、系统与软件安全、网络与通信安全、数据安全与个人信息保护和安全保障5个方面给出消费类智能门锁网络安全能力要求，由低到高按照基础级、增强级、领先级划分为三个等级，适用于指导消费类智能门锁的设计、开发、使用、维护和检测。

目　录

1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 概述 3
5 基础级要求 4
5.1 物理与硬件安全 4
5.2 系统与软件安全 5
5.3 网络与通信安全 11
5.4 数据安全与个人信息保护 11
5.5 安全保障 14
6 增强级要求 15
6.1 物理与硬件安全 15
6.2 系统与软件安全 15
6.3 网络与通信安全 18
6.4 数据安全与个人信息保护 18
6.5 安全保障 19
7 领先级要求 21
7.1 物理与硬件安全 21
7.2 系统与软件安全 21
7.3 网络与通信安全 23
7.4 数据安全与个人信息保护 24
7.5 安全保障 24
附录 A（规范性）不同安全能力等级的产品应符合的安全要求 26
附录 B（资料性）测试评价方法 28
B.1 基础级测评 28
B.2 增强级测评 53
B.3 领先级测评 68
附录 C（规范性）第三方检测机构能力要求 78
C.1 机构要求 78
C.2 人员要求 78
参　考　文　献 79

1 范围

本文件规定了消费类智能门锁网络安全标识基础级、增强级、领先级的网络安全能力要求，包括安全技术要求和安全保障要求。

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 21556.2—2025 锁具安全技术要求 第 2 部分：防盗锁

GB/T 25069—2022 信息安全技术 术语

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 38674—2020 信息安全技术 应用软件安全编程指南

GB/T 39276—2020 信息安全技术 网络产品和服务安全通用要求

GB/T 43741—2024 网络安全技术 网络安全众测服务要求

GB/T 44602—2024 网络安全技术 智能门锁网络安全技术规范

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

GB 46864—2025 数据安全技术 电子产品信息清除技术要求

3 术语和定义

3.1

消费类智能门锁　consumer smart lock products

消费者个人或组织可直接购买、使用，以生物特征、电子标签、近场无线通信、电子口令或远程控制指令等作为鉴别信息，具有互联网联网功能的门锁产品。

注：通常面向家庭和个人住宅场景。

3.2

关键安全参数　critical security parameter；CSP

与安全有关，其泄露或修改会危及密码模块安全的信息。

示例：秘密和私有密码密钥、口令之类的鉴别数据、个人标识码（PIN）、证书或其他信任锚。

注：消费类智能门锁中重点保护的关键安全参数包括设备根密钥、用户身份鉴别信息、设备鉴别信息、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

[来源：GB/T 25069—2022，有修改]

3.3

固件　firmware

功能上独立于主存储器，通常存储在只读存储器（ROM）中的指令和相关数据的有序集。

[来源：GB/T 25069—2022]

3.4

设备绑定　device binding

建立用户账号与消费类智能门锁间唯一权属关系的过程。

3.5

硬编码　hardcode

在编码过程中将可变变量用一个固定数值表示。

[来源：GB/T 38674—2020]

3.6

数字钥匙　digital key

用来控制智能门锁进行启、闭所使用的包含数字编码信息的载体。

注：消费类智能门锁的数字钥匙包括但不限于IC卡、智能手表、智能手机等包含数字编码信息的载体。

[来源：GB 21556.2—2025，有修改]

3.7

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。

[来源：GB/T 44602—2024]

4　概述

本文件从物理与硬件安全、系统与软件安全、网络与通信安全、数据安全与个人信息保护和安全保障5个方面构建消费类智能门锁安全框架（见图1）。

消费类智能门锁安全能力划分为三级，从基础级、增强级、领先

级逐级提升。基础级要求产品网络安全能力达到基本的网络安全水平，增强级要求产品网络安全能力达到同类产品先进水平，领先级要求产品网络安全能力达到同类产品领先水平。满足同一等级的所有适用的单项要求，方可获得该网络安全能力等级。各安全能力等级的产品应符合的安全要求见附录 A，测试评价方法参考附录 B。

开展基础级、增强级产品检测的第三方检测机构应满足附录 C.1 的要求；开展领先级产品检测的第三方检测机构应满足附录 C.1、C.2 的要求。

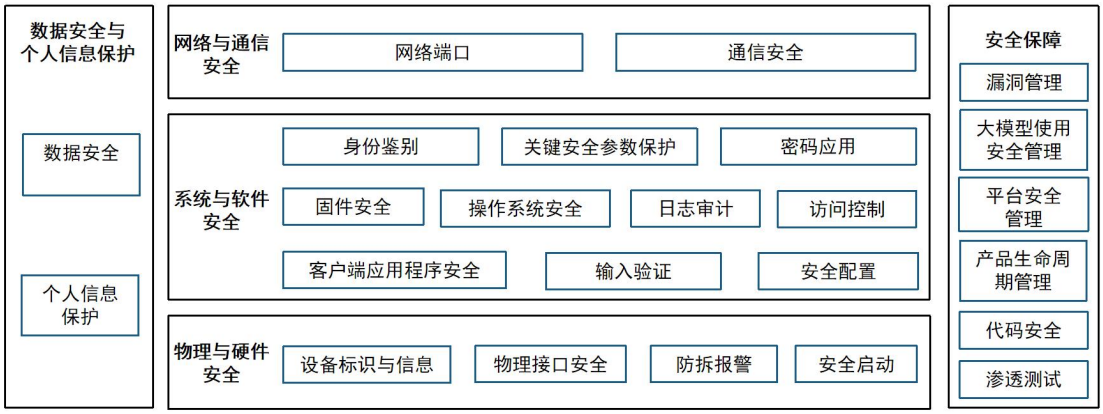


图1 消费类智能门锁安全框架

5 基础级要求

5.1 物理与硬件安全

5.1.1 设备标识与信息

消费类智能门锁应满足如下要求：

a) 具有唯一设备标识；

注：设备标识指用于识别或验证设备身份合法性的唯一标识符号。

b) 在设备外观清晰标识出设备型号、设备名称等信息。

5.1.2 物理接口安全

消费类智能门锁物理接口应满足如下要求:

a) 调试接口在出厂时设置为默认关闭;

b) 烧录接口、调试接口具备鉴别用户身份功能，仅由授权用户登录。

5.1.3 防拆报警

参照 GB 21556.2—2025 中 6.1.2.4 的要求，当拆除消费类智能门锁的防护面时，应能给出报警提示或发出报警信息。

5.2 系统与软件安全

5.2.1 身份鉴别

5.2.1.1 通用要求

消费类智能门锁应满足如下要求:

a) 对用户身份进行唯一标识，并采取防护措施防止标识被篡改;

b) 不存在未公开的账号和登录方式;

注：未公开的账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号。

c) 身份鉴别具备防暴力破解能力，参照 GB 21556.2—2025 中 6.1.2.3 输入错误报警的要求，在 5 min 内使用同一解锁方式累计错误次数达到阈值时，给出报警提示或发出报警信

息，同时该解锁方式自动进入无效输入状态，无效输入状态至少持续 90 s。

5.2.1.2 口令安全

消费类智能门锁使用口令进行身份鉴别时，应满足如下要求：

a) 具有口令复杂度要求，并限制口令最小长度；

注：口令复杂度包括但不限于限制连续升序、降序数字口令等；口令最小长度宜设置为6位及以上。

b) 出厂配置时采用默认口令登录设备的，默认口令在用户首次完成门锁初始化设置后失效；

c) 出厂配置时采用激活机制的，应在设备完成激活前拒绝激活以外的其他操作。通过用户设置口令进行设备激活的，应要求用户设置符合 5.2.1.2a）要求的口令；

注：激活指设备第一次使用时由用户采取相关操作才能使用设备的机制，包括设置口令、扫描二维码等。

d) 通过物理按键或其他安全方式将设备恢复到出厂设置后，应要求用户立即设置新口令，口令符合 5.2.1.2a）的要求；

注：恢复出厂设置的触发装置通常位于门锁内侧。

e) 口令在本地存储时，不以明文形式存储；

f) 口令在传输过程中使用安全协议非明文传输；

g) 能设置鉴别失败尝试次数阈值，鉴别失败超过设置的阈值后暂时锁定账户或触发告警。

5.2.1.3 生物特征识别安全

消费类智能门锁使用生物特征进行身份鉴别时，应满足如下要求：

a) 指纹识别功能符合 GB/T 44602—2024 中 6.1.1.2a）的要求，具备防复制指纹伪造、防指纹照片伪造的能力，能够抵御二维假体攻击；

b) 人脸识别功能符合 GB/T 44602—2024 中 6.1.1.2b）的要求，具备防复制人脸伪造、防人脸照片伪造、防纸质面具伪造的能力，能够抵御二维假体攻击；

c) 指/掌静脉、虹膜等其他类型生物特征识别功能具备防复制伪造、防照片伪造等二维假体呈现攻击的能力；

d) 发生以上类别攻击时具备相应的处理机制。

注：处理机制由制造商在使用说明书中定义，例如失败/错误提示，或进行风险提示等。

5.2.1.4 数字钥匙安全

消费类智能门锁使用数字钥匙进行近场身份鉴别时，应满足如下要求：

a) 采用密码技术保护数字钥匙内敏感数据，防止数据被窃取和滥用，并符合国家密码管理有关标准规范；

b) 智能门锁密钥应一机一密，单个设备绑定的数字钥匙应一钥一密；

c) 使用数字钥匙开锁时，应对数字钥匙中的认证数据进行解密校验，验证数字钥匙主体身份。

5.2.1.5 远程身份鉴别安全

消费类智能门锁提供远程管理功能时，应满足如下要求：

a) 通过网络登录设备进行管理操作时，对访问主体进行身份鉴别；

b) 使用数字证书进行身份鉴别的，设备的数字证书应和设备标识绑定。

5.2.2 关键安全参数保护

消费类智能门锁应满足如下要求：

a) 使用密码技术对关键安全参数进行机密性和完整性保护；

b) 不在设备软件代码中硬编码关键安全参数。

5.2.3 密码应用

消费类智能门锁中用于身份鉴别、安全更新、网络通信、数据存储、安全启动、关键安全参数保护等场景的加密技术应符合国家密码管理相关规定。

5.2.4 固件安全

消费类智能门锁固件应满足以下要求：

a) 固件更新具有授权机制，更新前应获得用户的授权；

b) 设备在第一次使用或恢复出厂设置后，检查更新并支持升级到最新版本；

c) 具备新的固件版本时，提示用户通过自动、人工方式进行安全更新，更新中止后能重新更新；

d) 固件下载应进行签名验证。下载完成后，应对下载文件进行完整性校验。如果验证失败，应拒绝更新并删除验证失败的固件程序；

e) 固件升级失败，具备固件回退能力，保持固件的可用性；

f) 采用安全机制，防止以未授权方式将固件回退到比当前版本更低的版本；

g) 采用安全保护机制，保护固件不能通过串口读取等非授权方式从硬件中提取出来；

h) 固件更新时，具备对更新文件来源进行校验的能力；

i) 固件及使用的第三方组件和开源软件不存在已公布的高风险安全漏洞。

5.2.5 操作系统安全

消费类智能门锁具备独立操作系统时，应满足最小化权限原则，仅为应用程序分配必要的权限。

5.2.6 日志审计

消费类智能门锁的日志审计功能，应满足如下要求：

a) 能对开关门锁、更改安全配置、管理用户、修改口令、登录失败、用户身份鉴别、通信会话中止、报警记录等用户在消费类智能门锁终端中的关键操作、重要行为、业务资源使用情况进行记录；

b) 审计日志包含事件的日期和时间、事件类型、操作用户和结果；

c) 本地审计记录具备存储容量保护措施，当存储空间超过阈值后，新审计记录覆盖旧审计记录，确保最新日志能正常记录，存储阈值参照 GB 21556.2—2025 的 6.1.2.5 中 A 级要求，本地存储数量不少于 32 条；

d) 仅允许授权用户访问审计日志。

5.2.7 访问控制

消费类智能门锁应满足如下要求：

a) 具有设备绑定功能的：

1) 在用户绑定设备时，与设备进行交互确认；

注：交互方式包括但不限于按键、蓝牙或无线网络配对、二维码等。

2) 已完成设备绑定的，仅接受来自绑定账号或其授权账号的控制指令；

3) 已完成设备绑定的，不再接受其它用户绑定，除非原设备绑定用户主动解除绑定。

b) 具有授权功能的：

1) 设备访问控制策略应满足最小授权原则，默认仅允许设备绑定用户访问受控资源或使用关键功能；

注：仅允许设备绑定用户更改访问控制策略，执行添加用户、删除用户等账户管理操作。

2) 仅允许设备绑定用户具备访问权限分享功能；

3) 采取防护措施保障分享的安全性。

注：保障分享的安全性防护措施包括但不限于分享权限即时回收、设置被分享者查看权限，宜设置分享有效期、被分享者水印等措施。

5.2.8 客户端应用程序安全

消费类智能门锁的客户端应用程序应符合 GB 21556.2—2025 中第 6.3 章节要求。

5.3 网络与通信安全

5.3.1 网络端口

消费类智能门锁的网络端口应满足如下要求：

a) 提供文档说明所有网络端口和服务，并告知对业务的影响；

b) 遵循最小配置原则，关闭非必要的通信端口。

5.3.2 通信安全

消费类智能门锁进行网络通信时，应满足如下要求：

a) 采用双向认证机制验证通信方身份；

b) 采用加密传输协议进行通信保护，防止传输过程中被窃听；

c) 具备通信完整性校验机制；

d) 发生通信延时或中断时，具备通信恢复机制。

5.4 数据安全与个人信息保护

5.4.1 数据安全

5.4.1.1 数据采集安全

消费类智能门锁采集数据时，应满足如下要求：

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，经用户同意后采集；

b) 数据采集时，采取最少必要原则，不过度采集；

c) 产品使用过程中，需要上传设备日志等相关信息进行故障诊断时，明确告知用户上传数据范围、目的和方式，经用户同意后上传；

d) 利用大模型处理用户数据的，需在采集前提前告知大模型处理的数据范围、目的和方式，并取得用户同意；

e) 具备语音交互功能的产品，具备静默状态下防窃听能力，应设置语音唤醒提示，通过物理灯光、声音应答或其它显著方式，即时告知用户设备处于语音信息采集状态，并支持用户关闭语音交互功能。

5.4.1.2 数据存储安全

消费类智能门锁存储数据时，应满足如下要求：

a) 具备数据保密性保护机制，采取加密方式对关键安全参数和敏感个人信息进行保护；

b) 具备数据完整性保护机制，防止对鉴别数据、审计日志的篡改删除；

c) 用户生物特征信息应在消费类智能门锁终端本地存储，不向云端或远程服务器传输，履行法定义务和法律法规另有规定的除外；

d) 具有断电信息保护机制，断电 24 h 后锁内保存的信息不应丢失。

5.4.1.3 数据销毁安全

消费类智能门锁应具备数据销毁机制，对废弃数据及时安全销毁。销毁数据前应明确提示用户，并由用户确认销毁后执行。数据销毁应符合 GB 46864—2025 的信息清除功能要求。

注：功能由产品或其管理端提供，用户自行使用。

5.4.2 个人信息保护

消费类智能门锁应满足如下要求：

a) 处理个人信息的，在产品管理相关界面、说明书等提供的链接页面公开展示个人信息处理规则，供用户查阅、复制或下载后查阅，规则内容包括但不限于：

1) 个人信息处理者的名称和联系方式；

2) 处理个人信息的种类和对应的处理目的、方式；

3) 明确个人信息是否存储在境内，以及存储的期限和到期后的处理方式；

4) 处理个人信息的必要性、对用户个人权益的影响和所采取安全措施的说明；

5) 查阅、复制、转移、更正、补充、删除用户个人信息，以及注销账号、撤回同意的方法和途径。

b) 个人信息收集应符合 GB/T 35273—2020 中第 5 章要求；

c) 个人信息存储应符合 GB/T 35273—2020 中第 6 章要求；

d) 未经用户同意，不应对所收集图片、视频中个人的身份进行关联分析，履行法定义务和法律法规另有规定的除外；

e) 处理用户敏感个人信息应符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

5.5 安全保障

5.5.1 漏洞管理

消费类智能门锁生产者应满足如下要求：

a) 确保设备不存在已知的高危及以上等级的漏洞；

注：已知高危漏洞参考 CNVD、CNNVD、NVDB 等国家级漏洞库。

b) 应明确并公示设备的型号，在规定或当事人约定期限内，持续进行安全更新；

c) 建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应；

d) 发现设备存在安全缺陷、漏洞时，应按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

5.5.2 大模型使用安全管理

消费类智能门锁利用大模型为用户提供服务的，所使用大模型应已通过生成式人工智能服务备案。

5.5.3 平台安全管理

消费类智能门锁的管理平台应通过网络安全等级保护二级及以上测评，并取得备案证明。

6 增强级要求

6.1 物理与硬件安全

6.1.1 设备标识与信息

在满足 5.1.1 的要求的同时，还应满足采取防护措施保护唯一设备标识不被篡改。

6.1.2 物理接口安全

应满足 5.1.2 的要求。

6.1.3 防拆报警

应满足 5.1.3 的要求。

6.1.4 安全启动

消费类智能门锁应默认具备安全启动机制，对设备固件和启动组件真实性和完整性进行校验通过后方可正常启动。

6.2 系统与软件安全

6.2.1 身份鉴别

6.2.1.1 通用要求

应满足 5.2.1.1 的要求。

6.2.1.2 口令安全

在满足 5.2.1.2 的要求的同时，还应满足如下要求：

a) 能识别并阻止口令重放攻击；

b) 键盘有震动或声音反馈时，按键引起的震动或声音无差异或随机反馈；

c) 提示用户定期更换口令，减少口令被破解的风险。

6.2.1.3 生物特征识别安全

在满足 5.2.1.3 的要求的同时，还应满足如下要求：

a) 指纹识别功能符合 GB/T 44602—2024 的 6.1.1.2d）中防 AI 深度合成伪造的要求；

b) 人脸识别功能符合 GB/T 44602—2024 的 6.1.1.2e）中防人脸视频伪造、防人脸电脑图像合成伪造、防 AI 深度合成伪造的要求；

c) 指/掌静脉、虹膜等其他类型生物特征识别功能具备防 AI 深度合成伪造等能力。

6.2.1.4 数字钥匙安全

在满足 5.2.1.4 的要求的同时，还应满足如下要求：

a) 通信时采用序列码、时间戳等机制，防御重放攻击；

b) 通信时采用相互鉴别机制，验证通信对方的身份。

6.2.1.5 远程身份鉴别安全

应满足 5.2.1.5 的要求。

6.2.2 关键安全参数保护

在满足 5.2.2 的要求的同时，还应满足如下要求：

a) 采用硬件方式保护设备根密钥；

注：硬件方式包括但不限于使用安全芯片、芯片的安全存储区等。

b) 建立规范的关键安全参数的安全管理流程；

注 1：管理对象包括但不限于根密钥，以及用于通信安全保护、安全更新保护、敏感个人信息保护的关键安全参数。

注 2：管理流程包括但不限于密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等。

c) 保证设备重要的关键安全参数对每个设备是唯一的。

6.2.3 密码应用

应满足 5.2.3 的要求。

6.2.4 固件安全

在满足 5.2.4 的要求的同时，消费类智能门锁固件中的关键代码和数据还应具备防篡改、防逆向能力。

6.2.5 操作系统安全

应满足 5.2.5 的要求。

6.2.6 日志审计

在满足 5.2.6 的要求的同时，还应参照 GB 21556.2—2025 的 6.1.2.5 中 B 级要求，本地记录存储数量不少于 500 条。

6.2.7 访问控制

应满足 5.2.7 的要求。

6.2.8 客户端应用程序安全

应满足 5.2.8 的要求。

6.2.9 输入验证

消费类智能门锁应对通过用户界面输入、应用程序编程接口输入的数据进行安全验证，以避免数据处理过程中出现意外行为。

注：数据处理过程中出现的意外行为包括但不限于SQL注入、操作系统命令注入和路径遍历等。

6.2.10 安全配置

消费类智能门锁应默认提供安全的配置，并向用户提供安全设置的指导。

6.3 网络与通信安全

6.3.1 网络端口

在满足 5.3.1 的要求的同时，还需满足如下要求：

a) 未认证状态下减少网络端口暴露信息；

b) 用户可关闭非必要的网络服务。

6.3.2 通信安全

在满足 5.3.2 的要求的同时，还应满足在传输通道加密的基础上，对应用层敏感个人信息进行端到端加密，确保中间节点无法获取内容明文。

6.4 数据安全与个人信息保护

6.4.1 数据安全

在满足 5.4.1 的要求的同时，还应满足断电 168 h 后锁内保存的信息不丢失。

6.4.2 个人信息保护

在满足 5.4.2 的要求的同时，还应满足如下要求：

a) 个人信息处理规则中涉及收集和向其他个人信息处理者提供个人信息的目的、方式、种类以及接收方信息的，以清单等形式予以列明；

b) 用户通过管理端交互界面等便捷通道行使个人信息权利的，不得设置不合理条件限制用户的合理请求。

6.5 安全保障

6.5.1 漏洞管理

应满足 5.5.1 的要求。

6.5.2 大模型使用安全管理

应满足 5.5.2 的要求。

6.5.3 平台安全管理

消费类智能门锁的管理平台应通过网络安全等级保护三级及以上测评，并取得备案证明。

6.5.4 产品生命周期管理

消费类智能门锁产品生命周期管理应满足如下要求：

a) 建立产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节；

b) 建立产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁；

c) 编制开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程；

d) 建立产品安全开发机制，满足 GB/T 39276—2020 第 5.1.2.1 项相关要求；

e) 建立安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等；

f) 建立安全交付机制，在产品交付和重要版本发布前进行安全审查和加固，包括但不限于：

1) 删除非必要的账号、测试账号；

2) 从发布的版本中删除所有调试代码；

3) 禁用不必要的物理接口、网络服务、网络端口、网络接口；

4) 启用消费类智能门锁的安全功能，包括身份鉴别、访问控制、数据加密等功能。

g) 建立安全运维机制和流程，满足 GB/T 39276—2020 第 5.2.2.3 项相关要求。

6.5.5 代码安全

消费类智能门锁生产者应满足如下要求:

a) 建立开源代码来源审查机制，使用开源组件和开源软件的，确保开源代码来源可信;

b) 应建立开源代码安全漏洞跟踪和处置机制，对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

7 领先级要求

7.1 物理与硬件安全

7.1.1 设备标识与信息

应满足 6.1.1 的要求。

7.1.2 物理接口安全

应满足 6.1.2 的要求。

7.1.3 防拆报警

应满足 6.1.3 的要求。

7.1.4 安全启动

应满足 6.1.4 的要求。

7.2 系统与软件安全

7.2.1 身份鉴别

7.2.1.1 通用要求

应满足 6.2.1.1 的要求。

7.2.1.2 口令安全

在满足 6.2.1.2 的要求的同时，应具备虚位口令功能，以适应不同场景下的防窥需求。

7.2.1.3 生物特征识别安全

在满足 6.2.1.3 的要求的同时，还应满足如下要求:

a) 指纹识别功能符合 GB/T 44602—2024 的 6.1.1.2d）中防假体指纹伪造的要求，能够抵御三维假体攻击;

b) 人脸识别功能符合 GB/T 44602—2024 的 6.1.1.2e）中防假体面具伪造的要求，能够抵御三维假体攻击;

c) 指/掌静脉、虹膜等其他类型生物特征识别功能具备防假体伪造等呈现攻击的能力，能够抵御三维假体攻击。

7.2.1.4 数字钥匙安全

在满足 6.2.1.4 的要求的同时，应满足如下要求：

a) 具备防止复制能力;

b) 具备防范中继攻击的能力。

7.2.1.5 远程身份鉴别安全

应满足 6.2.1.5 的要求。

7.2.2 关键安全参数保护

在满足 6.2.2 的要求的同时，还应满足采用通过国密二级认证的安全芯片保护设备根密钥和用户身份鉴别信息。

7.2.3 密码应用

应满足 6.2.3 的要求。

7.2.4 固件安全

应满足 6.2.4 的要求。

7.2.5 操作系统安全

应满足 6.2.5 的要求。

7.2.6 日志审计

应满足 6.2.6 的要求。

7.2.7 访问控制

应满足 6.2.7 的要求。

7.2.8 客户端应用程序安全

应满足 6.2.8 的要求。

7.2.9 输入验证

应满足 6.2.9 的要求。

7.2.10 安全配置

应满足 6.2.10 的要求。

7.3 网络与通信安全

7.3.1 网络端口

应满足 6.3.1 的要求。

7.3.2 通信安全

应满足 6.3.2 的要求。

7.4 数据安全与个人信息保护

7.4.1 数据安全

应满足 6.4.1 的要求。

7.4.2 个人信息保护

应满足 6.4.2 的要求。

7.5 安全保障

7.5.1 漏洞管理

应满足 6.5.1 的要求。

7.5.2 大模型使用安全管理

应满足 6.5.2 的要求。

7.5.3 平台安全管理

应满足 6.5.3 的要求。

7.5.4 产品生命周期管理

应满足 6.5.4 的要求。

7.5.5 代码安全

在满足 6.5.5 的要求的同时，消费类智能门锁生产者还应满足如下要求：

a) 委托第三方检测机构针对设备自身代码进行检测，确保软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误；

b) 使用应用程序对设备进行管理的，委托第三方检测机构针对设备管理应用程序进行检测，确保软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误。

7.5.6 渗透测试

消费类智能门锁生产者应委托众测平台开展网络安全众测，并满足如下要求：

a) 测试时间应不少于 14 天，发现高危及以上级别漏洞，测试立即终止，本轮测试结束；

b) 参与测试主体不少于 20 个，且具备相关领域漏洞发现能力，以及相关领域漏洞发现项目经验；

c) 对测试中发现的可被利用的中危漏洞进行修复，经众测平台确认后，获得网络安全众测报告。

附录 A

（规范性）

不同安全能力等级的产品应符合的安全要求

表A.1列出了消费类智能门锁基础级、增强级和领先级应符合的安全要求。

表A.1 不同安全能力等级的产品应符合的安全要求

技术要求		基础级要求对应章条号	增强级要求对应章条号	领先级要求对应章条号
物理与硬件安全	设备标识与信息	5.1.1	6.1.1	7.1.1
	物理接口安全	5.1.2	6.1.2	7.1.2
	防拆报警	5.1.3	6.1.3	7.1.3
	安全启动	—	6.1.4	7.1.4
系统与软件安全	身份鉴别	5.2.1	6.2.1	7.2.1
	关键安全参数保护	5.2.2	6.2.2	7.2.2
	密码应用	5.2.3	6.2.3	7.2.3
	固件安全	5.2.4	6.2.4	7.2.4
	操作系统安全	5.2.5	6.2.5	7.2.5
	日志审计	5.2.6	6.2.6	7.2.6
	访问控制	5.2.7	6.2.7	7.2.7
	客户端应用程序安全	5.2.8	6.2.8	7.2.8
	输入验证	—	6.2.9	7.2.9
	安全配置	—	6.2.10	7.2.10
网络与通信安全	网络端口	5.3.1	6.3.1	7.3.1
	通信安全	5.3.2	6.3.2	7.3.2
数据安全与个人信息保护	数据安全	5.4.1	6.4.1	7.4.1
	个人信息保护	5.4.2	6.4.2	7.4.2
安全保障	漏洞管理	5.5.1	6.5.1	7.5.1
	大模型使用安全管理	5.5.2	6.5.2	7.5.2
	平台安全管理	5.5.3	6.5.3	7.5.3
	产品生命周期	—	6.5.4	7.5.4

	管理			
	代码安全	—	6.5.5	7.5.5
	渗透测试	—	—	7.5.6

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC

附录 B
（资料性）
测试评价方法

B.1 基础级测评

B.1.1 物理与硬件安全

B.1.1.1 设备标识与信息

设备标识与信息的测评方法如下：

a) 测试方法：

1) 检查设备标识是否具有保证设备标识唯一性的说明；尝试通过管理界面、接口、平台等对设备标识进行修改；

2) 检查设备外观的名称、型号等信息是否清晰；核查用户配置界面、管理 APP 等位置的相关信息是否与外观一致。

b) 预期结果：

1) 设备具有保证设备标识唯一性的说明；

2) 设备外观清晰标识出设备的名称、型号等信息，并且与用户配置界面、管理 APP 等位置的信息一致；无法对唯一性标识进行修改。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.1.2 物理接口安全

消费类智能门锁物理接口安全测评方法和预期结果如下：

a) 测评方法：

1) 查看调试接口，是否在出厂时设置为默认关闭；

2) 查看烧录接口、调试接口是否具备鉴别用户身份功能，是否仅由授权用户登录。

b) 预期结果：

1) 调试接口在出厂时设置为默认关闭；

2) 烧录接口、调试接口具备鉴别用户身份功能，仅由授权用户登录。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.1.3 防拆报警

防拆报警的测评方法如下：

a) 测试方法：

消费类智能门锁处于正常工作状态时，查验拆除防护面是否给出报警提示或发出报警信息。

b) 预期结果:

消费类智能门锁处于正常工作状态时，拆除防护面给出报警提示或发出报警信息。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2 系统与软件安全

B.1.2.1 身份鉴别

B.1.2.1.1 通用要求

通用要求测评方法如下:

a) 测试方法:

1) 检查唯一标识生成算法，分析是否存在防止标识被篡改的防护措施;

2) 查阅产品说明文档，检查产品中是否存在未公开的账号和登录方式，账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键;

3) 查看产品说明文档，记录产品支持的所有解锁方式，针对每种解锁方式，使用未授权的凭证在 5 min 内连续进行错误输入操作，错误登录超过设定次数后，检查是否进入报警状态，并用秒表记录无效输入状态的

持续时间是否不少于 90 s。

b) 预期结果:

1) 产品对用户身份进行唯一标识，并采取防护措施防止标识被篡改;

2) 产品中不存在未公开的账号和登录方式，账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键;

3) 产品具备防暴力破解能力，规定时间内鉴别失败超过设置的阈值后能触发报警，并进入无效输入状态。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.1.2 口令安全

口令安全的测评方法如下:

a) 测试方法:

1) 查看产品是否具有口令复杂度配置功能（例如：不应使用连续升序、降序数字等复杂度要求），验证策略是否生效，查看产品是否限制口令最小长度，验证策略是否生效;

2) 根据产品说明文档，查看出厂设备的初始口令。如果初始口令为默认口令的，验证用户首次登录时是否提

示更改默认口令，初始口令在用户注册后是否失效；

3) 检查出厂配置时采用激活机制的产品，是否在设备完成激活前拒绝激活以外的其他操作，是否存在与激活无关的暴露面，如网络端口、物理接口等。通过用户设置口令进行设备激活的产品，是否要求用户设置复杂度符合 5.2.1.2a）要求的口令；

4) 通过物理按键或其他安全方式重新设置口令，或将设备恢复到出厂设置状态，并检查是否要求用户立即设置新口令，口令要求是否符合 5.2.1.2a）的要求；

5) 查看口令本地存储文件，验证口令是否以明文形式存储；

6) 抓包验证口令在传输过程中是否使用安全协议非明文传输；

7) 查验用户是否能设置鉴别失败尝试次数阈值，鉴别失败超过设置的阈值后是否暂时锁定账户或触发告警。

b) 预期结果：

1) 产品具有口令复杂度配置功能，能配置口令组成字符类型，不能使用简单或容易猜测的口令，并限制口令最小长度，策略生效；

2) 出厂配置时采用默认口令登录设备的，默认口令在用户首次完成门锁初始化设置后失效；

3) 出厂配置时采用激活机制的产品，在完成激活前拒绝激活以外的其他操作。通过用户设置口令进行设备激活的产品，用户设置符合 5.2.1.2a）要求的口令;

4) 通过物理按键或其他安全方式将设备恢复到出厂设置状态时，要求用户立即设置新口令，口令符合 5.2.1.2a）的要求;

5) 口令本地存储文件中口令以非明文形式存储;

6) 口令在传输过程中使用安全协议非明文传输;

7) 用户能设置鉴别失败尝试次数阈值，鉴别失败超过设置的阈值后暂时锁定账户或触发告警。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.1.3 生物特征识别安全

生物特征识别安全的测评方法如下:

a) 测试方法:

1) 查看指纹识别模块是否具备防复制指纹伪造、防指纹照片伪造的能力，是否符合 GB/T 44602—2024 中 6.1.1.2a）的要求;

2) 查看人脸识别模块是否具备防复制人脸伪造、防人脸照片伪造、防纸质面具伪造的能力，是否符合 GB/T

44602—2024 中 6.1.1.2b）的要求；

3) 查看指/掌静脉、虹膜等其他类型生物识别模块是否具备防复制伪造、防照片伪造等呈现攻击的能力；

4) 查看发生上述攻击时生物特征识别模块是否具备相应的处理机制。

b) 预期结果：

1) 指纹识别模块具备防复制指纹伪造、防指纹照片伪造的能力，符合 GB/T 44602—2024 中 6.1.1.2a）的要求；

2) 人脸识别模块具备防复制人脸伪造、防人脸照片伪造、防纸质面具伪造的能力，符合 GB/T 44602—2024 中 6.1.1.2b）的要求；

3) 指/掌静脉、虹膜等其他类型生物识别模块具备防复制伪造、防照片伪造等呈现攻击的能力；

4) 发生上述攻击时生物特征识别模块具备相应的处理机制。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.1.4 数字钥匙安全

数字钥匙安全的测评方法如下：

a) 测试方法：

1) 读取不同受试产品中数字钥匙存储的信息，验证是否采用密码技术对存储的敏感信息（包括密钥和用户数据）进行加密处理，是否符合国家密码管理有关标准规范；

2) 查看不同数字钥匙的密钥是否不同；

3) 检查受试样品程序中是否有对数字钥匙进行校验的程序/流程。

b) 预期结果：

1) 采用密码技术对数字钥匙内存储的敏感信息进行加密处理，符合国家密码管理有关标准规范；

2) 单个设备绑定的数字钥匙实现一钥一密；

3) 使用数字钥匙开锁时进行了数字钥匙合法性认证，对数字钥匙中的认证数据进行解密校验。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.1.5 远程身份鉴别安全

远程身份鉴别的测评方法如下：

a) 测试方法：

1) 查阅产品说明文档，检查核对设备所有网络端口、管理应用程序等网络登录方式，是否都需要身份鉴别；

2) 使用数字证书进行身份鉴别的，查阅产品说明文档，设备的数字证书是否和设备标识绑定。

b) 测试方法：

1) 所有通过网络登录设备的方式，都对访问主体进行身份鉴别；

2) 使用数字证书进行身份鉴别的，设备的数字证书和设备标识绑定。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.2 关键安全参数保护

关键安全参数保护的测评方法如下：

a) 测试方法：

1) 查阅产品设计文档，检查是否采用了密码技术对关键安全参数进行保护；

2) 查看设备软件代码，检查代码中是否存在硬编码的关键安全参数。

b) 预期结果：

1) 产品使用了密码技术对关键安全参数进行保护；

2) 设备软件代码中不存在硬编码的关键安全参数。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.3 密码应用

密码应用的测评方法如下：

a) 测试方法：

查阅设备设计文档，确认身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术是否符合国家密码管理相关规定。

b) 预期结果：

身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术符合国家密码管理相关规定。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.4 固件安全

固件安全的测评方法如下：

a) 测试方法：

1) 查看被测样品是否具有自动、手动更新功能，对于自动更新功能，检查更新前是否需要授权用户自动更新；对于手动更新功能，检查更新前是否需要用户授权下载更新和安装；

2) 查阅设备说明文档，检查设备是否在第一次使用或恢复出厂设置后，检查更新并支持升级到最新版本；

3) 验证当被测样品检测到具有新的固件版本时，是否提示用户通过自动或人工方式进行更新；并验证更新流程在主动取消、通信中断等异常中止场景下，设备保持安全可用状态，可正常重新发起升级，且重新更新时仍执行完整固件签名校验；

4) 使用未经签名验证的固件，在授权的条件下进行系统更新，检查受试样品是否拒绝进行更新并删除验证失败的固件程序；修改固件升级文件的内容，在授权的条件下进行系统更新，检查设备是否拒绝进行更新并删除验证失败的固件程序；

5) 固件升级失败时，验证产品是否具备固件回退能力，回退到升级前的版本，保持固件的可用性；

6) 查阅设备说明文档，查验产品是否采用安全机制，防止以未授权方式将固件回退到比当前版本更低的版本，尝试非授权更新低版本固件，验证是否成功；

7) 查阅硬件及设计文档，核查产品所采用的安全保护机制（如 MCU 调试接口鉴权、Flash 读保护、禁用调试下载接口等），验证固件不能通过串口、调试接口等非授权方式从硬件中提取出来；

8) 尝试固件更新，验证是否具备对更新文件来源进行校验的能力；

9) 使用漏洞扫描工具进行漏洞扫描，查看固件及使用的第三方组件和开源软件是否存在已公布的高风险安全漏洞。

b) 预期结果：

1) 固件更新具有授权机制，更新前应获得用户授权；

2) 设备在第一次使用或恢复出厂设置后，检查更新并支持升级到最新版本；

3) 具备新的固件版本时，提示用户通过自动、人工方式进行安全更新，更新中止后可重新更新；

4) 固件下载需进行签名验证，并在下载完成后进行完整性校验。如果验证失败，拒绝更新并删除验证失败的固件程序；

5) 固件升级失败时，具备固件回退能力，保持固件的可用性；

6) 产品采用安全机制，防止以未授权方式将固件回退到比当前版本更低的版本；

7) 产品采用安全保护机制，保护固件不能通过串口读取等非授权方式从硬件中提取出来；

8) 固件更新时，具备对更新文件来源进行校验的能力；

9) 固件及使用的第三方组件和开源软件不存在已公布的高风险安全漏洞。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.5 操作系统安全

操作系统安全的测评方法如下。

a) 测评方法:

查看智能门锁终端操作系统的应用程序信息,是否满足最小化原则。

b) 预期结果:

智能门锁终端操作系统的应用程序权限满足最小化原则。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.6 日志审计

日志审计的测评方法如下。

a) 测试方法:

1) 当用户对智能门锁终端进行操作时，查看对于关键操作、重要行为、业务资源使用情况是否进行日志记录，内容包括但不限于：开关门锁、更改安全配置、管理

用户、修改口令、登录失败、用户身份鉴别、通信会话中止、报警记录等；

2) 查看审计日志是否包含事件的日期和时间、事件的类型、操作用户和结果；

3) 对记录存储上限进行测试，检查审计日志是否具有保护措施，保障日志存储量超过阈值后审计日志正常记录；并验证本地存储记录数量，是否不少于32条；

4) 验证是否仅允许授权用户访问审计日志。

b) 预期结果：

1) 产品对用户的关键操作、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：开关门锁、更改安全配置、管理用户、修改口令、登录失败、用户身份鉴别、通信会话中止、报警记录等；

2) 审计日志包含事件的日期和时间、事件的类型、操作用户和结果；

3) 智能门锁终端对本地审计日志记录具有保护措施，日志存储量超过阈值后审计日志能正常记录，且本地日志存储数量不少于32条；

4) 仅允许授权用户访问审计日志。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况

判定为“不符合”。

B.1.2.7 访问控制

访问控制的测评方法如下：

a) 测试方法：

1) 具有设备绑定功能的产品：

(1) 查阅产品设计文档，核验用户在绑定设备时，是否与设备进行交互确认；

(2) 核验已完成设备绑定的产品，是否可以接受来自绑定账号或其授权账号的控制指令；

(3) 核验已完成设备绑定的产品，是否可以在原设备绑定用户未主动解除绑定的情况下，接受其它用户的绑定。

2) 具有授权功能的产品：

(1) 查阅产品设计文档，检查访问控制策略是否满足最小授权原则，是否仅允许设备绑定用户访问受控资源或使用关键功能；

(2) 非设备绑定用户尝试使用访问权限分享功能，验证是否能访问成功；

(3) 查阅产品设计文档，检查是否采取防护措施保障分享的安全性。

b) 预期结果：

1) 具有设备绑定功能的产品：

(1) 在用户绑定设备时，与设备进行交互确认；

(2) 已完成设备绑定的产品，仅接受来自绑定账号或其授权账号的控制指令；

(3) 已完成设备绑定的，不再接受其它用户绑定，除非原设备绑定用户主动解除绑定。

2) 具有授权功能的产品：

(1) 设备访问控制策略满足最小授权原则，仅允许设备绑定用户访问受控资源或使用关键功能；

(2) 仅设备绑定用户具备访问权限分享功能，其它用户不具备权限分享功能；

(3) 产品具备防护措施保障分享的安全性。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.8 客户端应用程序安全

客户端应用程序安全的测评方法如下：

a) 测试方法：

参考 GB 21556.2—2025 中第 8.4 章节客户端应用程序安全试验的要求开展测试。

b) 预期结果：

消费类智能门锁客户端应用程序符合GB 21556.2—2025中第6.3章节要求。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.3 网络与通信安全

B.1.3.1 网络端口

网络端口的测评方法如下:

a) 测试方法:

1) 进入设备管理界面，查阅设备文档，确认是否完整说明所有网络端口的用途及对应服务;

2) 扫描智能门锁终端，核验是否开启业务需求以外的通信端口。

b) 预期结果:

1) 设备提供了文档并说明所有网络端口和服务;

2) 智能门锁终端遵循最小配置原则，已关闭非必要的通信端口。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.3.2 通信安全

通信安全的测评方法如下:

a) 测试方法:

1) 使用网络封包分析软件获取受试样品的网络通信数据包，并进行分析，验证是否采用双向鉴别机制向其接入的网络证明其网络身份;

2) 抓包查看数据传输过程中是否采取加密传输协议等措施对通信进行保护;

3) 使用网络封包分析软件获取受试样品的网络通信数据包，并进行分析，查看数据包中是否具有校验传输数据完整性的校验数据，验证校验机制是否生效;

4) 断开网络连接 30 min 后恢复网络连接，验证智能门锁产品是否具备通信延时或中断的恢复机制。

b) 预期结果:

1) 采用双向鉴别机制向其接入的网络证明其网络身份;

2) 采取了加密传输协议进行通信保护;

3) 产品具备传输完整性的校验机制;

4) 产品具备通信延时或中断的恢复机制。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4 数据安全与个人信息保护

B.1.4.1 数据安全

B.1.4.1.1 数据采集安全

数据采集安全的测评方法如下:

a) 测试方法:

1) 数据采集前，查验用户手册、用户通知、隐私协议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，数据采集范围是否遵循最小必要原则;

3) 查验上传设备日志的情况时，是否明确告知用户上传数据范围、目的和方式，并经用户同意后上传;

4) 如产品使用大模型处理用户信息的，查验用户手册、用户通知、隐私协议等信息中是否告知用户大模型处理的数据范围、目的和方式，并取得用户同意;

5) 查验具备语音交互功能的产品，是否具备静默状态下防窃听能力，是否设置语音唤醒提示，如通过物理灯光提示、声音应答或其它显著方式，即时告知用户处于语音信息采集状态，是否支持用户关闭语音交互功能。

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；

3) 上传设备日志等相关信息进行故障诊断时，明确告知了用户上传数据范围、目的和方式，并经用户同意后上传；

4) 利用大模型处理用户数据的，在采集前已提前告知用户大模型处理的数据范围、目的和方式，并取得用户同意；

5) 具备语音交互功能的产品，具备静默状态下防窃听能力，已设置语音唤醒提示，即时告知用户处于语音信息采集状态，支持用户关闭语音交互功能。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4.1.2 数据存储安全

数据存储安全的测评方法如下：

a) 测试方法：

1) 查看智能门锁终端数据，是否对存储的关键安全参数和敏感个人信息进行加密处理；

2) 查看智能门锁终端鉴别数据、审计数据是否可通过外

部操作方式进行篡改删除；

3) 查验用户生物特征信息是否存储在智能门锁终端设备本地，未向云端或远程服务器传输（法定情形除外）；

4) 验证终端断电后 24 h，锁内信息是否丢失。

b) 预期结果：

1) 智能门锁终端存储的敏感信息进行了加密处理；

2) 智能门锁终端存储的鉴别数据、审计数据具备完整性保护机制；

3) 将用户生物特征信息存储在智能门锁终端设备本地，不向云端或远程服务器传输；

4) 具备断电信息保护机制，断电 24 h 后锁内保存的信息未丢失。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4.1.3 数据销毁安全

数据销毁安全的测评方法如下：

a) 测试方法：

查看智能门锁终端是否具备数据销毁机制，是否对废弃数据及时安全销毁，是否有残留数据，销毁数据前是否明确提示用户，并由用户确认销毁后执行。

b) 预期结果：

智能门锁终端具备数据销毁机制，能对废弃数据及时安全销毁，无残留数据，销毁数据前明确提示用户，并由用户确认销毁后执行。产品的数据销毁为用户提供符合 GB 46864—2025 要求的信息清除功能，以简单便捷的方式从设备中删除数据。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4.2 个人信息保护

个人信息保护的测评方法如下：

a) 测试方法：

1) 检查产品管理相关界面、说明书、外包装盒等载体确认是否提供个人信息处理规则的访问入口或明确链接，验证是否提供在线查阅、复制文本或下载功能；核查处理规则内容是否符合 5.4.2a）的要求；

2) 审查产品的个人信息收集流程，核查收集的个人信息种类；验证同意的可撤回性，审查产品是否存在未经用户同意，通过隐蔽方式（如后台静默收集）获取个人信息的情况；

3) 审查产品个人信息处理规则、隐私政策等文档，核查

存储期限的合理性，检查存储方式的安全性，验证跨境存储合规性，敏感个人信息的传输和存储的合规性；

4) 检查是否存在未经用户同意，对图片、视频中个人身份进行关联分析的情况（法定情形除外）；

5) 审查产品个人信息处理规则，处理用户敏感个人信息是否符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

b) 预期结果：

1) 产品提供了个人信息处理规则并符合 5.4.2a）的要求；

2) 产品个人信息收集符合 GB/T 35273—2020 中第 5 章的要求；

3) 产品个人信息存储符合 GB/T 35273—2020 中第 6 章的要求；

4) 设备不存在未经用户单独同意对所收集图片、视频中个人的身份进行关联分析行为；

5) 处理用户敏感个人信息符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.5 安全保障

B.1.5.1 漏洞管理

漏洞管理的测评方法如下:

a) 测试方法:

1) 检查产品所有漏洞，核查产品是否存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及以上级别漏洞;

2) 检查产品生产者是否明确并公示设备的型号，验证产品是否在规定或当事人约定期限内持续进行安全更新，核查产品是否建立和执行产品安全缺陷、漏洞的应急响应机制和流程，并对在运行和维护阶段发现的安全缺陷、漏洞进行响应;

3) 检查产品生产者管理制度和相关文件，是否建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

4) 检查产品生产者管理制度和相关文件，是否在发现设备存在安全缺陷、漏洞时，按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

b) 预期结果:

1) 产品不存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及高危以上级别漏洞;

2) 产品明确并公示设备的型号，持续进行安全更新，建立和执行产品安全缺陷、漏洞的应急响应机制和流程，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

3) 建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

4) 发现安全缺陷、漏洞时，产品立即按照国家网络安全监测预警和信息通报制度等相关规定采取修复或替代方案等补救措施，并及时告知用户安全风险，向有关主管部门报告。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.5.2 大模型使用安全管理

大模型使用安全管理的测评方法如下:

a) 测试方法:

如利用大模型为用户提供服务的，查阅有关材料，验证消费类智能门锁使用的大模型是否已通过生成式人工智能服

务备案。

b) 预期结果：

利用大模型为用户提供服务的，所使用大模型应已通过生成式人工智能服务备案。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.5.3 平台安全管理

平台安全管理的测评方法如下：

a) 测试方法：

查验被测方提供的相关证明材料，验证消费类智能门锁的管理平台是否通过网络安全等级保护二级及以上测评，取得备案证明。

b) 预期结果：

消费类智能门锁管理平台通过了网络安全等级保护二级及以上测评，并取得备案证明。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2 增强级测评

B.2.1 物理与硬件安全

B.2.1.1 设备标识与信息

在满足 B.1.1.1 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定:

a) 测试方法:

检查产品是否采取防护措施保护唯一标识不被篡改，审查产品设计文档，确认唯一设备标识的存储位置及防篡改机制。

b) 预期结果:

产品采取防护措施保护唯一标识不被篡改。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.1.2 物理接口安全

应满足 B.1.1.2 的测评方法。

B.2.1.3 防拆报警

应满足 B.1.1.3 的测评方法。

B.2.1.4 安全启动

安全启动的测评方法如下:

a) 测试方法:

检查消费类智能门锁是否具备安全启动机制，是否对固件

和启动组件的真实性和完整性进行校验；核查校验后产品的安全启动机制能否正常启动。

b) 预期结果：

产品实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验通过后方可正常启动。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2 系统与软件安全

B.2.2.1 身份鉴别

B.2.2.1.1 通用要求

应满足 B.1.2.1.1 的测评方法。

B.2.2.1.2 口令安全

在满足 B.1.2.1.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 验证产品是否具有识别并阻止口令重放攻击的机制，例如使用一次性令牌或时间戳；

2) 键盘有震动或声音反馈时，验证按键引起的震动或声音是否无差异或随机反馈；

3) 验证产品是否提示用户定期更换口令。

b) 预期结果：

1) 产品具有识别并阻止口令重放攻击的机制；

2) 键盘有震动或声音反馈时，按键引起的震动或声音无差异或随机反馈；

3) 产品具有提示用户定期更换口令的功能。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.1.3 生物特征识别安全

在满足 B.1.2.1.3 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查看并验证指纹识别模块是否符合 GB/T 44602—2024 的 6.1.1.2d）中防 AI 深度合成伪造的要求；

2) 查看并验证人脸识别模块是否符合 GB/T 44602—2024 的 6.1.1.2e）中防人脸视频伪造、防人脸电脑图像合成伪造、防 AI 深度合成伪造的要求；

3) 查看并验证指/掌静脉、虹膜等其他类型生物特征识别功能是否具备防 AI 深度合成伪造等呈现攻击的能力。

b) 预期结果：

1) 指纹识别模块符合 GB/T 44602—2024 的 6.1.1.2d）中防 AI 深度合成伪造的要求；

2) 人脸识别模块符合 GB/T 44602—2024 的 6.1.1.2e）中防人脸视频伪造、防人脸电脑图像合成伪造、防 AI 深度合成伪造的要求；

3) 指/掌静脉、虹膜等其他类型生物特征识别功能具备防 AI 深度合成伪造等呈现攻击的能力。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.1.4 数字钥匙安全

在满足 B.1.2.1.4 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 通过抓包等方式验证通信时是否采用序列码、时间戳等机制，防御重放攻击；

2) 通过抓包等方式验证通信时是否采用相互鉴别机制，验证通信对方的身份。

b) 预期结果：

1) 通信时采用序列码、时间戳等机制，防御重放攻击；

2) 通信时采用相互鉴别机制，验证通信对方的身份。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.1.5 远程身份鉴别安全

应满足 B.1.2.1.5 的测评方法。

B.2.2.2 关键安全参数保护

在满足 B.1.2.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查阅产品设计文档，检查是否采用了硬件方式对设备根密钥进行保护；

2) 查阅产品设计文档，检查是否建立了规范的关键安全参数的安全管理流程，例如密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等；

3) 查阅产品设计文档，检查是否保证设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

b) 预期结果：

1) 产品采用了硬件方式对设备根密钥进行保护；

2) 建立了规范的关键安全参数的安全管理流程；

3) 设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.3 密码应用

应满足 B.1.2.3 的测评方法。

B.2.2.4 固件安全

在满足 B.1.2.4 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

验证固件中的关键代码和数据是否具备防篡改、防逆向能力。

b) 预期结果：

固件中的关键代码和数据具备防篡改、防逆向能力。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.5 操作系统安全

应满足 B.1.2.5 的测评方法。

B.2.2.6 日志审计

在满足 B.1.2.6 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定:

a) 测试方法:

验证本地存储记录数量，是否不少于 500 条。

b) 预期结果:

本地日志存储数量不少于 500 条。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.7 访问控制

应满足 B.1.2.7 的测评方法。

B.2.2.8 客户端应用程序安全

应满足 B.1.2.8 的测评方法。

B.2.2.9 输入验证

输入验证的测评方法如下:

a) 测试方法:

查阅设备设计文档，检查是否存在对通过用户界面输入、应用程序编程接口输入的数据的安全校验措施。在用户界

面输入框中提交非法字符，验证系统是否拦截非法输入，且未向后端传输无效数据。

b) 预期结果：

存在对通过用户界面输入、应用程序编程接口输入的数据的安全校验措施，系统可以拦截非法输入。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.10 安全配置

安全配置的测评方法如下：

a) 测试方法：

查看设备管理操作界面或控制应用程序界面，核查设备是否提供设备配置项列表，是否默认为安全的，所有网络服务、端口为默认最小化的；查看设备配置过程，核查设备是否向用户进行安全设置的指导。

b) 预期结果：

设备提供默认安全的配置，向用户提供安全设置的指导。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.3 网络与通信安全

B.2.3.1 网络端口

网络端口的测评方法如下:

a) 测试方法:

1) 未登录认证时，查看网络端口暴露的信息是否简化;

2) 验证是否可手动关闭非必要的网络服务。

b) 预期结果:

1) 设备未认证状态下未暴露网络端口信息;

2) 用户可关闭非必要的网络服务。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.3.2 通信安全

通信安全的测评方法如下:

a) 测试方法:

验证在传输通道加密的基础上，是否对应用层敏感数据进行端到端加密，在客户端与服务器之间使用预置的公私钥对建立 TLS 连接，在中间节点启用 TLS 解密功能，在客户端触发一个包含敏感个人信息的报文后，在已配置的中间节点捕获该操作产生的所有网络流量，解密后的 TLS 流量中的应用层数据，检查其中包含的敏感个人信息字段是否

加密。

b) 预期结果：

在传输通道加密的基础上，对应用层敏感数据进行端到端加密，确保中间节点无法获取内容明文。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4 数据安全与个人信息保护

B.2.4.1 数据安全

在满足 B.1.4.1 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

验证消费类智能门锁断电后 168 h，锁内信息是否丢失。

b) 预期结果：

消费类智能门锁断电 168 h 后锁内保存的信息不丢失。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4.2 个人信息保护

在满足 B.1.4.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查阅个人信息处理规则，确认对外提供个人信息的目的、方式、种类及接收方是否以清单形式列明；

2) 验证管理端是否有便捷通道（如设置页、客服入口）供用户行使个人信息权利，是否设置不合理限制条件。

b) 预期结果：

1) 设备对外提供个人信息相关内容以清单形式清晰列明；

2) 设备有便捷通道（如设置页、客服入口）供用户行使个人信息权利，无不合理限制条件。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5 安全保障

B.2.5.1 漏洞管理

应满足 B.1.5.1 的测评方法。

B.2.5.2 大模型使用安全管理

应满足 B.1.5.2 的测评方法。

B.2.5.3 平台安全管理

平台安全管理的测评方法如下：

a) 测试方法：

查验被测方提供的相关证明材料，验证消费类智能门锁的

管理平台是否通过网络安全等级保护三级及以上测评，并取得备案证明。

b) 预期结果：

消费类智能门锁的管理平台通过了网络安全等级保护测评三级及以上测评，并取得备案证明。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5.4 产品生命周期安全管理

生命周期安全管理测评方法如下：

a) 测试方法：

1) 查阅产品管理文档，确认是否建立覆盖设计、开发、测试、交付、运维等环节的全生命周期网络安全管理机制；

2) 核查安全设计机制文档，是否参考 GB/T 39276—2020 第 5.1.2.1 项进行威胁建模，包含威胁识别、分析及缓解措施；

3) 查看开发安全文档，是否描述设计和开发过程中保障数据存储与传输机密性、完整性的机制和流程；

4) 核查安全开发机制相关文件，是否满足 GB/T 39276—2020 第 5.1.2.1 项要求；

5) 查阅安全测试机制文档及测试记录，确认定期或在重要版本发布前是否开展静态安全测试、动态安全测试等规定测试类型；

6) 检查安全交付机制文档及交付记录，确认产品交付和重要版本发布前是否执行安全审查和加固；

7) 核查安全运维机制和流程文档，是否满足 GB/T 39276—2020 第 5.2.2.3 项要求。

b) 预期结果：

1) 产品生产者建立了产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节；

2) 产品生产者建立了产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁；

3) 产品生产者编制了开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程；

4) 产品生产者建立了产品安全开发机制，应满足 GB/T 39276—2020 第 5.1.2.1 项相关要求；

5) 产品生产者建立了安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等；

6) 产品生产者建立了安全交付机制，在产品交付和重要版本发布前进行安全审查和加固；

7) 产品生产者建立安全运维机制和流程，应满足 GB/T 39276—2020 第 5.2.2.3 项相关要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5.5 代码安全

代码安全的测评方法如下：

a) 测试方法：

1) 查验是否建立开源代码来源审查机制，使用开源组件和开源软件的，验证开源代码来源是否可信；

2) 查验是否建立开源代码安全漏洞跟踪和处置机制，对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

b) 预期结果：

1) 建立了开源代码来源审查机制，使用开源组件和开源软件的，开源代码来源可信；

2) 建立了开源代码安全漏洞跟踪和处置机制，对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3 领先级测评

B.3.1 物理与硬件安全

B.3.1.1 设备标识与信息

应满足 B.2.1.1 的测评方法。

B.3.1.2 物理接口安全

应满足 B.2.1.2 的测评方法。

B.3.1.3 防拆报警

应满足 B.2.1.3 的测评方法。

B.3.1.4 安全启动

应满足 B.2.1.4 的测评方法。

B.3.2 系统与软件安全

B.3.2.1 身份鉴别

B.3.2.1.1 通用要求

应满足 B.2.2.1.1 的测评方法。

B.3.2.1.2 口令安全

在满足 B.2.2.1.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

检查消费类智能门锁是否具备虚位口令功能，尝试输入一串符合要求的虚位口令，验证是否能开启门锁。

b) 预期结果：

智能门锁产品具备虚位口令功能。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.1.3 生物特征识别安全

在满足 B.2.2.1.3 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查看指纹识别模块是否符合 GB/T 44602—2024 的 6.1.1.2d）中防假体指纹伪造的要求；

2) 查看人脸识别模块是否符合 GB/T 44602—2024 的 6.1.1.2e）中的防假体面具伪造的要求；

3) 查看对指/掌静脉、虹膜等其他类型生物特征识别功能是否具备防假体伪造等模拟呈现攻击的能力。

b) 预期结果：

1) 指纹识别模块符合 GB/T 44602—2024 的 6.1.1.2d）中防假体指纹伪造的要求；

2) 人脸识别模块符合 GB/T 44602—2024 的 6.1.1.2e）中防假体面具伪造的要求；

3) 指/掌静脉、虹膜等其他类型生物特征识别功能具备防假体伪造等呈现攻击的能力。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.1.4 数字钥匙安全

在满足 B.2.2.1.4 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查阅产品数字钥匙安全设计文档、通信协议方案，梳理钥匙下发、身份鉴别、数据存储与读写机制；检索公开漏洞库、安全文献，排查已知数字钥匙复制漏洞（如静态凭证克隆、全局固定密钥、无随机数/计数器的报文重放、弱密钥派生缺陷、密钥明文存储、仅校验 UID 不校验签名等）；基于梳理的攻击面，采用识别到的各类复制手段开展数字钥匙复制测试；使用复制得到的数字钥匙尝试执行解锁操作，验证产品是否具备防范数字钥匙复制的能力并记录结果；

2) 查阅产品数字钥匙安全设计文档，梳理防止中继攻击

相关防护方案，如是否存在距离边界校验、往返时延校验、二次用户交互验证等阻断中继攻击的技术手段；

3) 使用中继攻击模拟设备搭建攻击链路，模拟中间人远程转发数字钥匙信号开展实测，验证中继攻击相关防护方案；

4) 记录中继攻击场景下门锁是否会非法解锁、是否触发异常告警。

b) 预期结果：

1) 数字钥匙具备防复制能力；

2) 满足至少 1 项阻断中继攻击的技术手段，证明设备具备防范中继攻击的能力。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.1.5 远程身份鉴别安全

应满足 B.2.2.1.5 的测评方法。

B.3.2.2 关键安全参数保护

在满足 B.2.2.2 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定：

a) 测试方法：

查看智能门锁产品密码算法与芯片对应证书，检查是否采

用通过国密二级认证的安全芯片保护设备根密钥和用户身份鉴别信息。

b) 预期结果:

设备采用通过国密二级认证的安全芯片保护设备根密钥和用户身份鉴别信息。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.3 密码应用

应满足 B.2.2.3 的测评方法。

B.3.2.4 固件安全

应满足 B.2.2.4 的测评方法。

B.3.2.5 操作系统安全

应满足 B.2.2.5 的测评方法。

B.3.2.6 日志审计

应满足 B.2.2.6 的测评方法。

B.3.2.7 访问控制

应满足 B.2.2.7 的测评方法。

B.3.2.8 客户端应用程序安全

应满足 B.2.2.8 的测评方法。

B.3.2.9 输入验证

应满足 B.2.2.9 的测评方法。

B.3.2.10 安全配置

应满足 B.2.2.10 的测评方法。

B.3.3 网络与通信安全

B.3.3.1 网络端口

应满足 B.2.3.1 的测评方法。

B.3.3.2 通信安全

应满足 B.2.3.2 的测评方法。

B.3.4 数据安全与个人信息保护

B.3.4.1 数据安全

应满足 B.2.4.1 的测评方法。

B.3.4.2 个人信息保护

应满足 B.2.4.2 的测评方法。

B.3.5 安全保障

B.3.5.1 漏洞管理

应满足 B.2.5.1 的测评方法。

B.3.5.2 大模型使用安全管理

应满足 B.2.5.2 的测评方法。

B.3.5.3 平台安全管理

应满足 B.2.5.3 的测评方法。

B.3.5.4 产品生命周期管理

应满足 B.2.5.4 的测评方法。

B.3.5.5 代码安全

在满足 B.2.5.5 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定:

a) 测试方法:

1) 查阅第三方检测机构出具的代码检测报告，检测对象为源代码或二进制程序，验证软件、第三方库和第三方组件中是否存在中危及以上安全漏洞、是否存在硬编码身份鉴别信息和关键安全参数等错误；确认检测机构具备相应检测资质，检测流程符合规范;

2) 核查产品是否存在使用应用程序进行设备管理的情况;若存在，查阅第三方检测机构出具的设备管理应用程序检测报告，检测对象为源代码或二进制程序，验证软件、第三方库和第三方组件中是否存在中危及以上安全漏洞、是否存在硬编码身份鉴别信息和关键安全参数等错误；确认检测机构具备相应检测资质，检测流程符合规范;

3) 核查检测报告中的检测过程记录、原始数据及检测结论，确认检测内容无遗漏、检测方法科学合理，检测结果真实有效。

b) 预期结果：

1) 委托第三方检测的，检测机构具备相应资质；对设备自身代码进行全面检测，软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误；

2) 使用应用程序对设备进行管理的，应委托第三方对设备管理应用程序进行全面检测，检测机构具备相应资质；软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误；

3) 检测报告完整规范，包含检测资质证明、检测流程、检测内容、检测数据、检测结论等核心要素，检测过程符合相关标准要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.5.6 渗透测试

消费类智能门锁生产者应委托众测平台开展网络安全众测，并满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 由众测平台搭建的隔离仿真测试环境，测试时间不少

于 14 天，参与测试主体（推荐包含智能体）不少于 20 个，执行完整六阶段众测流程；

2) 终端设备测试应包含硬件接口、外置存储、设备固件、OTA 升级程序；开展物理硬件安全、系统软件安全测试，覆盖安全启动、口令鉴别、固件安全、访问控制、日志审计等安全维度；设备管理应用程序测试应包含测试身份认证、会话管理、本地数据存储、输入校验、敏感信息保护等；还应包含设备、配套 app 与管理平台的数据传输、身份认证、权限服务等；

3) 测试过程中如发现高危及以上级别漏洞，测试立即终止，本轮测试结束；测试过程中发现的可被利用的中危漏洞，厂商进行修复，并交众测平台进行确认。

b) 预期结果：

1) 由众测平台搭建的隔离仿真测试环境，测试时间不少于 14 天，参与测试主体不少于 20 个，执行完整六阶段众测流程；

2) 在测试中未发现高危漏洞，发现的可被利用的中危漏洞厂商均已进行修复，并经平台确认；

3) 检测报告完整规范，包含检测资质证明、检测流程、检测内容、检测数据、检测结论等核心要素，检测过程符合相关标准要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

附录 C
（规范性）
第三方检测机构能力要求

C.1 机构要求

第三方检测机构应满足如下要求：取得检验检测机构资质认定(CMA)，或通过中国合格评定国家认可委员会(CNAS)实验室认可，CMA 批准的检验检测能力范围或 CNAS 认可能力范围涵盖网络安全检测相关内容。

C.2 人员要求

进行渗透测试的第三方检测机构应至少有 5 人专职从事渗透测试相关工作，相关人员应至少满足下列章条中的任意 1 项要求：

a) 具有 CISP-PTE、CISP-PTS 等渗透测试相关证书；

b) 具有渗透测试相关项目经历；

c) 具有 5 年内通过合法方式挖掘安全漏洞并向国家权威漏洞库报送的经历；

d) 在国家级、省部级、市区级（或行业级）网络安全赛事获得奖励的人员。

参 考 文 献

[1] GB/T 38626—2020 信息安全技术 智能联网设备口令保护指南

[2] GB/T 38632—2020 信息安全技术 智能音视频采集设备应用安全要求

[3] GB/T 39720—2020 信息安全技术 移动智能终端安全技术要求及测试评价方法

[4] GB/T 41387—2022 信息安全技术 智能家居通用安全规范

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC