ICS 35.240.01
CCS L67

团　　体　　标　　准

T/CAQI 287—2022

家用和类似用途智能门锁生物识别安全性评价要求

Technology specification for household and similar intelligent door locks security on biometrics system

2022 - 12 - 06 发布　　2022 - 12 - 16 实施

中国质量检验协会 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。

本文件由厦门立林科技有限公司提出

本文件由中国质量检验协会归口。

本文件起草单位：南京市产品质量监督检验院（南京市质量发展与先进技术应用研究院）、厦门立林科技有限公司、奥普家居股份有限公司、珠海格力电器股份有限公司、深圳绿米联创科技有限公司、厦门狄耐克智能科技股份有限公司、广东顶固集创家居股份有限公司、深圳市依蒙科技集团有限公司、王力安防科技股份有限公司、圣点世纪科技股份有限公司、安钥(北京)科技股份有限公司、杭州萤石软件有限公司、福州物联网开放实验室有限公司、浙江威欧希科技股份有限公司、广东必达保安系统有限公司、深圳市柯尼斯智能科技有限公司、广东好太太科技集团股份有限公司、深圳市凯迪仕智能科技股份有限公司、杭州华橙网络科技有限公司、松下电气机器（北京）有限公司、佛山照明智达电工科技有限公司、安徽扬子安防股份有限公司、广东亚太天能科技股份有限公司、亚亚（广东）锁业科技有限公司、北京中标信科技术服务有限公司。

本文件主要起草人：郭梦伊、张谦、张心予、段卉冰、张辉、张桓、黄培强、黄伟、支崇铮、胡文矛、陈其嘤、官世武、张天辰、周烨、吴劲勇、徐跃祥、周亮、李显、童川、马国华、潘锦洪、周宝龙、庄伟、顾学亚、王淑艳。

家用和类似用途智能门锁生物识别安全性评价要求

1 范围

本文件规定了家用和类似用途智能门锁生物特征识别安全性评价指标体系及安全等级、评价指标和测评方法。

本文件适用于民用及商用建筑的智能门锁生物识别安全水平评价，不适用于工业和特殊用途生物智能锁具的相关评价。

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 25069-2022 信息安全技术 术语
GB/T 34975-2017 信息安全技术 移动智能终端 应用软件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 35735-2017 公共安全 指纹识别应用 采集设备通用技术要求
GB/T 35783-2017 信息技术 虹膜识别设备通用规范
GB/T 37742-2019 信息技术 生物特征识别 指纹识别设备通用规范
GB/T 40660-2021 信息安全技术 生物特征识别信息保护基本要求
GA 374-2019 电子防盗锁
GA/T 893-2010 安防生物特征识别应用术语
GA/T 938-2012 安防指静脉识别应用系统设备通用技术要求
GA/T 1179-2014 安防声纹确认应用算法技术要求和测试方法
GA/T 1212-2014 安防人脸识别应用 防假体攻击测试方法
SJ/T 11608-2016 人脸识别设备通用规范

3 术语和定义

GB/T 25069-2010、GA 374-2019和GA/T 893-2010界定的以及下列术语和定义适用于本文件。

3.1

智能门锁 intelligent door locks

在本体上以电子方式识别并处理生物特征、电子信息、无线遥控编码、网络通讯等信息，控制机械执行机构实施启闭及远程信息传输的锁具。

3.2

管理平台 management platform

为智能门锁提供接入、绑定、查询等的信息服务系统。

3.3

认假率 false accept rate

将来自非授权用户的测试样本误认做授权用户的比率。

3.4

拒真率 false reject rate

将来自授权用户的测试样本误认做非授权用户的比率。

3.5

安全评价 security assessment

以实现智能门锁生物识别安全为目的，对智能门锁应用中可能存在的安全风险进行识别分析和评估的过程。

3.6

活体指纹 living fingerprint

具有人体温度、导电性等生物特征的指表皮上凸起的纹线。

3.7

安全指数 security index

用于表征智能门锁生物识别安全水平高低的一组数字和字母的组合，智能门锁个数达到相应等级的智能效用和对应的安全等级的组成。

4 技术要求

4.1 功能安全

4.1.1 要求

智能门锁应能对生物特征进行采集和特征数据提取，并具备唯一编号，注册存储其生物特征数据；应能辨识已进行生物特征注册用户的身份，并能拒绝未注册用户；应能支持对已进行生物特征注册用户的特征模板与生物特征数据进行删除操作。

4.1.2 评分规则

满分 30 分，不具备此功能得 0 分，实际得分计算:$30 \times a_1 \times b_1 \times c_1 \times d_1 \times e_1$（圆整到整数位），其中：

a）仅活体指纹才能开锁（100%），三维立体且导电的指纹即能开锁（80%），三维立体指纹即能开锁（50%），不具备此功能（100%），记为 a_1；

b）仅活体人脸才能开锁（100%），仿真人脸面具即能开锁（80%），人脸视频或人脸照片即能开锁（50%）,不具备此功能（100%），记为 b_1；

c）仅真实虹膜才能开锁（100%），复制虹膜纹理的隐形眼镜或虹膜组织高仿材料等形式的假体能开锁（80%），虹膜照片、虹膜视频即能开锁（50%），不具备此功能（100%），记为 c_1；

d）仅真实指静脉才能开锁（100%），实体手指绘制指静脉纹路或穿戴指套，或指静脉指模能开锁（80%）,复制指静脉纹理的二维静态或动态图像即能开锁（50%），不具备此功能（100%），记为 d_1；

e）仅真实声纹用户才能开锁（100%），语音模仿、语音转换合成、录音重放和录音拼接能开锁（80%）,不具备此功能（100%），记为 e_1。

4.2 识别方式安全

4.2.1 认假率

认假率 FAR=被系统接受的非授权用户测试样本数/总的非授权用户测试样本数 × 100%。

4.2.2 拒真率

拒真率 FRR=被系统拒绝的授权用户测试样本数/总的授权用户测试样本数×100%。

4.2.3 要求

不同识别方式安全的认假率和拒真率指标应满足表 1 要求。

表 1 不同识别方式的认假率 FAR 和拒真率 FRR 的要求

项目		要求	
		认假率（%）	拒真率（%）
指纹识别	一般级	≤0.001	≤5
	增强级	≤0.001	≤3
人脸识别	一般级	≤0.001	≤1
	增强级	≤0.0001	≤1
虹膜识别	一般级	≤0.01	≤1
	增强级	≤0.001	≤1
指静脉识别	一般级	≤0.01	≤1
	增强级	≤0.001	≤3
声纹识别	一般级	≤2	≤2
	增强级	≤1	≤2

4.2.4 评分规则

满分 30 分，实际得分计算:$30 \times a_2$（圆整到整数位），其中：

符合增强级（100%），符合一般级（80%），记为 a_2。

4.3 本地信息保存安全

4.3.1 要求

智能门锁应对本地个人信息进行加密处理。

4.3.2 评分规则

满分 20 分，不具备此项功能得 0 分，实际得分计算：$20 \times a_3$（圆整到整数位），其中：

在信息加密的基础上对本地个人生物识别信息加密，且加密密钥满足一机一密，数据应时效性，具备抗攻击能力（100%）。仅对本地个人信息进行加密处理，未对个人生物识别信息进行再次加密（80%），记为 a_3。

4.4 通信安全

4.4.1 要求

具有联网功能的智能门锁终端、移动应用和管理平台各执行主体在收集和传输个人生物特征数据时，应同时满足以下要求：

a)个人生物特征识别信息应满足 GB/T 40660-2021 的要求,个人信息范围应符合 GB/T 35273-2020 的要求。

b）应采用密码技术保证通信过程中数据的完整性；

c）采用不同通信协议时，应采用相应的技术以防止中间人攻击。

4.4.2 评分规则

满分 10 分，不具备此功能得 0 分。实际得分计算:$10 \times a_4$（圆整到整数位）,其中满足要求（100%），否则（0%），记为 a_4。

4.5 固件安全

4.5.1 要求

具有联网功能的智能门锁，应符合下列要求：

a）应具备固件升级功能；

b）固件升级应校验固件文件的签名信息；

c）若通过硬件接口形式进行固件升级，需在说明书中明示，若以 OTA 方式升级，则升级操作需经用户授权同意；

d）由于断电断网或其他原因导致联网模块固件升级失败，重新上电后联网模块仍应可以正常工作。

4.5.2 评分规则

满分 10 分，不具备此功能得 0 分，实际得分计算:$10 \times a_5 \times b_5 \times c_5$（圆整到整数位），其中：

a）提示用户升级并需用户确认（100%），否则（80%），记为 a_5；

b）断电断网后重新上电可以正常工作（100%），否则（0%），记为 b_5；

c）能够查询联网模块固件版本信息（100%），否则（80%），记为 c_5。

4.6 移动应用安全

4.6.1 要求

具有移动应用的智能门锁应满足 GB/T 34975-2017 中对移动智能终端应用软件安全功能和安全保障的要求，以防御篡改攻击。

4.6.2 评分规则

满分 20 分，不具备此功能得 0 分，实际得分计算:$20 \times a_6$（圆整到整数位）,其中满足要求（100%），否则（0%），记为 a_6。

4.7 多生物特征识别

4.7.1 要求

智能门锁除具备多种单独开锁模式外，宜能通过采集多模态或多生物特征，对用户进行注册、识别、添加和删除等操作，并同时满足 4.2 的要求。

4.7.2 评分规则

满分 30 分，不具备此功能得 0 分，实际得分计算:$30 \times a_7 \times b_7$（圆整到整数位），其中：

a）可设置任意两种或以上生物特征识别组合开锁模式（100%），只能采用特定组合模式开锁（80%），记为 a_7；

b）各种生物特征识别开锁系统相互独立，不受其它开锁系统故障的影响（100%），否则（70%），记为 b_7。

4.8 监测与报警功能

4.8.1 要求

智能门锁应能够监测周围环境并在发现异常时发出警报的功能。

4.7.2 评分规则

评分规则：满分 20 分，实际得分计算:$20 \times a_8 \times b_8$（圆整到整数位），其中：

a）联网锁具有防劫持报警功能，当输入设定好的被劫持生物特征时，手机 APP/PC 端发出报警（100%）,否则（80%），记为 a_8；

b）除“防劫持报警”外，联网锁本体和手机 APP/PC 端能够同步显示报警（100%），否则（80%），记为 b_8。

5 试验方法

5.1 试验条件

除特别声明环境条件的试验外，试验应在下列环境条件下进行：

——环境温度：15℃～35℃；

——相对湿度：45%～75%；

——大气压强：86kPa～106kPa；

本测试在同一样品上进行，如果试验失败或门锁损坏，则启用备样测试。

5.2 功能安全

依据以下步骤执行试验程序：

a)指纹：按 GB/T 35735-2017 中 6.3 的规定进行，判定试验过程中及试验后结果是否符合 4.1.1 的要求。

b)人脸：按 GA/T 1212-2014 的规定进行，判定试验过程中及试验后结果是否符合 4.1.1 的要求。

c)虹膜：按 GB/T 35783-2017 中 5.4 的规定进行，判定试验过程中及试验后结果是否符合 4.1.1 的要求。

d)指静脉：按 GA/T 938-2012 中 5.3 的规定进行，判定试验过程中及试验后结果是否符合 4.1.1 的要求。

e)声纹：按 GA/T 1179-20147 中 5 的规定进行，判定试验过程中及试验后结果是否符合 4.1.1 的要求。

判定准则按 4.1.2 的规定进行。

5.3 识别方式安全

依据以下步骤执行试验程序：

a)指纹识别：按GB/T 37742-2019中7.5.4的规定进行，判定试验过程中及试验后结果是否符合4.2.3的要求。

b)人脸识别：按 SJ/T 11608-2016 中 6.4.3 的规定进行，判定试验过程中及试验后结果是否符合 4.2.3 的要求。

c)虹膜识别：按GB/T 35783-2017中5.5.6的规定进行，判定试验过程中及试验后结果是否符合4.2.3的要求。

d)指静脉：按 GA/T 938-2012 中 5.4 的规定进行，判定试验过程中及试验后结果是否符合 4.2.3 的要求。

e)声纹：按 GA/T 1179-2014 中 5.4.1 的规定进行，判定试验过程中及试验后结果是否符合 4.2.3 的要求。

判定准则按 4.2.4 的规定进行。

5.4 本地信息保存安全

5.4.1 试验材料及工具

智能门锁，电源或电池，信息安全测评工具。

5.4.2 试验程序

依据以下步骤顺序执行试验程序：

a) 将门锁安装好并接通电源；

b) 按制造商文件规定的安全级别，使用信息安全测评工具测试智能门锁本地是否利用密码技术对个人信息和个人生物识别信息进行加密。

5.4.3 监测数据

本地个人信息的加密处理情况。

5.4.4 判定准则

按 4.3.2 的规定进行。

5.5 通信安全

5.5.1 试验材料及工具

智能门锁，电源或电池，手机或 iPad 等远程控制终端，稳定网络的环境，信息安全测评工具，说明书，门锁的联网模块、远程控制终端能够连接上互联网，并且与服务器之间通信正常，网速不低 500Kbps。

5.5.2 试验程序

依据以下步骤顺序执行试验程序：

a）根据说明书功能，操作智能门锁、移动应用和管理平台，检查在收集、存储和使用个人生物特征识别信息时是否需满足 5.5.1 的要求。

b）使用信息安全测评工具测试智能门锁终端、移动应用和管理平台，通过抓包工具通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证；

c）查看系统在通信过程中，对整个报文或会话过程是否进行加密。判定其结果是否符合 4.4.1 的要求。

5.5.3 监测数据

个人生物特征识别信息满足 GB/T 40660-2021 的要求；采用密码技术保证通信过程中数据的完整性；采用不同通信协议时，采用相应的技术以防止中间人攻击。

5.5.4 判定准则

按 4.4.2 的规定进行。

5.6 固件安全

5.6.1 试验材料及工具

智能门锁，电源或电池，手机或 iPad 等远程控制终端，稳定网络的环境，门锁的联网模块、远程控制终端能够连接上互联网，并且与服务器之间通信正常，网速不低 500Kbps。

5.6.2 试验程序

依据以下步骤顺序执行试验程序：

a）将门锁安装好并接通电源；

b）服务器挂载两个联网模块固件程序，保证版本号不一样，可做测试升级切换。

5.6.3 监测数据

APP 能够显示当前联网模块固件版本信息，最新固件版本信息，升级时有进度提示，升级完成后显示升级完成信息。也可通过后台服务器监测联网模块升级状态信息。

5.6.4 判定准则

按 4.5.2 的规定进行。

5.7 移动应用安全

按 GB/T 34975-2017 的规定进行，判定试验过程中及试验后结果是否符合 4.6.1 的要求。判定准则按 4.6.2 的规定进行。

5.8 多生物特征识别

5.8.1 试验材料及工具

智能门锁，电源或电池，万用表。

5.8.2 试验程序

依据以下步骤顺序执行试验程序：

a）将门锁安装好并接通电源；

b）依次用门锁支持的开锁方式进行解锁；

c）依据门锁说明书检查是否可任意组合两种生物特征开锁模式，若可以，将所支持的所有开锁模式进行两两组合，进行开锁；

d）若规定了特定的组合方式，则只试验规定的组合进行开锁；

e）依据门锁说明书检查生物特征开锁系统是否独立，若相互独立，每次失效一个开锁系统，测试其它系统能否正常开锁。

5.8.3 监测数据

组合开锁的组合方式；开锁系统间的独立性。

5.8.4 判定准则

按 4.7.2 的规定进行。

5.9 监测与报警功能

5.9.1 试验材料及工具

智能门锁，电源或电池。

5.9.2 试验程序

依据以下步骤顺序执行试验程序：

a）将门锁安装好并接通电源；

b）依次利用门锁所支持的生物识别开锁方式的无效指令连续进行开锁，达到厂家声明的次数，检查门锁及 APP 反馈响应；

c）录入防劫持生物特征纹，然后输入该生物特征，检查门锁及 APP 反馈响应。

5.9.3 监测数据

以上每种情况下的门锁本体和远程控制端 APP 的反馈响应。

5.9.4 判定准则

按 4.8.2 的规定进行。

6 评价指标和安全等级

6.1评价指标

评价指标应根据安全评价要素，按表2确定。

表2 智能门锁生物识别安全性评价技术要求和判定准则对应关系

序号	安全评价项目	安全评价要素	技术要求 条款号	判定准则 条款号	分值
1	功能安全	保密、完整、可用	4.1.1	5.2	30
2	识别方式安全	保密、完整、可用	4.2.3	5.3	30
3	本地信息保存安全	保密、完整	4.3.1	5.4.4	20

4	通信安全	保密、完整	4.4.1	5.5.4	10
5	固件安全	保密、完整	4.5.1	5.6.4	10
6	移动应用安全	保密、完整、可用	4.6.1	5.7	20
7	多生物特征识别	保密、可用	4.7.1	5.8.4	30
8	监测与报警功能	保密、可用	4.8.1	5.9.4	20
注：智能门锁各项安全评价项目的实际得分根据表中“安全评价要素”一列的分布，分别累加到相应的各个安全评价要素总分，例如“功能安全”实际得分20分，则“保密”、“完整”、“可用”三个安全评价要素方面分别累计20分。					

6.2安全等级

安全等级应根据生物识别方式和每项评价项目实际得分，按表3确定。

表3 智能门锁生物识别安全等级判定

评价要素	识别方式	安全等级	
		B级	A级
保密	指纹识别/人脸识别/虹膜识别/指静脉识别/声纹识别（按实际情况选择）	> 135	85 ~ 135
完整		> 95	60 ~ 95
可用		> 105	65 ~ 105