ICS 67.140.10
CCS X 55

团　　体　　标　　准

T/OIDAA x—xxxx

实名制的智能门锁系统个人信息保护实施指南

Implementation guidelines for personal information protection of real-name smart lock system

（草案）

（本稿完成日期：2024-12-23）

xxxx-xx-xx 发布　　xxxx-xx-xx 实施

中关村安信网络身份认证产业联盟　　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。

本文件由中关村安信网络身份认证产业联盟提出。

本文件起草单位：兴唐通信科技有限公司、北京海鑫智圣技术有限公司、厦门中盾安信科技有限公司、北京中电华大电子设计有限责任公司、杭州闪易科技有限公司、四川长虹电器股份有限公司、中国信息通信研究院、海十联（上海）智能科技有限公司。

本文件主要起草人：许雪姣、蔡子凡、贺银苹、姜文昊、王剑冰、温扬睿、金鑫、于克兵、邹骁、马俊、杨震泉、黄德俊、庞伟伟、张立锋、周建。

引　言

在旅馆、日租房（网约房）等场景下的实名登记工作中，为落实《旅馆业治安管理办法》《旅馆业治安管理条例》等政策规定，满足《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》等法律对智能门锁系统中个人身份认证过程所涉及的个人信息保护、个人信息监管要求，增强旅馆、日租房（网约房）等场景下智能门锁应用的合规性，降低个人信息泄露、个人信息滥用等安全风险，对智能门锁行业进行良性引导，特制定本文件。

实名制的智能门锁系统个人信息保护实施指南

1 范围

本文件提供了实名制的智能门锁系统个人信息保护实施指南。

本文件适用于旅馆、日租房（网约房）等场景下的智能门锁系统个人身份认证服务。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35678—2017 公共安全 人脸识别应用 图像技术要求

GB/T 37076—2018 信息安全技术 指纹识别系统技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GB/T 42574—2023 信息安全技术 个人信息处理中告知和同意的实施指南

GA/T 467—2019 居民身份证验证安全控制模块接口技术规范

GA/T 1723.4—2020 居民身份网络认证 认证服务 第4部分：人脸图像采集控件技术要求

GM/T 0028—2014 密码模块安全技术要求

T/OIDAA 01—2024 智能门锁系统个人身份认证服务基本功能规范

3 术语和定义

T/OIDAA 01-2024 界定的术语和定义适用于本文件。

4 总则

4.1 系统参考模型

实名制的智能门锁系统由智能门锁管理平台和智能门锁组成：

——智能门锁管理平台主要实现对预订信息、入住信息、密钥的管理及对智能门锁的接入认证和安全连接；

——智能门锁主要实现身份信息的收集、认证、接受远程控制、控制门锁开启和关闭、数据记录功能。

智能门锁系统的外部相关方本文件不进行指导，可能涉及：

——预订系统：预订系统是对互联网预订平台、酒店/网约房业务平台的抽象化逻辑实体；

——居民身份网络认证服务系统：作为智能门锁系统的支撑，完成个人身份认证服务；

——居民身份证相关系统：完成实名身份的认证服务；

——监管系统。监管系统是有关部门的相关系统，主要负责接收由智能门锁系统上报的用户信息，可以实现流动人口动、静态信息的全面管理，必要时将用户信息作为追溯依据。

个人信息在实名制的智能门锁系统中主要包括姓名、身份信息摘要、身份信息密文、网络标识、居民身份网络可信凭证、生物特征信息、公民身份号码、手机号等敏感个人

信息和身份信息，及在访问门锁业务时涉及到的门锁标识、用户口令信息、用户权限设置信息、门锁与用户的绑定关系信息、用户开锁信息、密钥信息等。

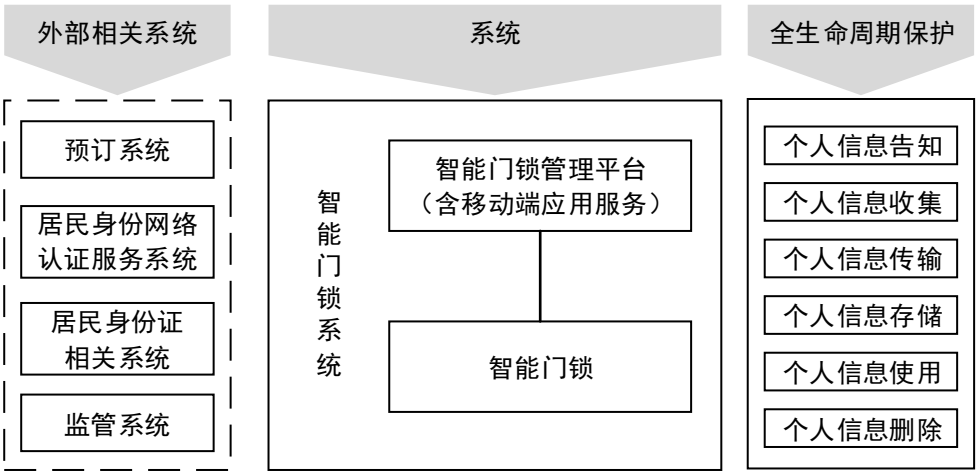

图 1 实名制的智能门锁系统个人信息保护参考框架图

实名制的智能门锁系统个人信息保护主要涉及个人信息的告知、收集、传输、存储、使用和删除过程。

4.2 安全目标

实名制的智能门锁系统个人信息保护实施过程中使用密码技术对个人信息进行机密性、完整性、真实性和不可否认性保护。在需要同时保证个人信息的机密性和完整性时,先对个人信息进行完整性保护,再对个人信息进行机密性保护。具体实施方法包括但不限于：

——个人信息机密性保护。采用数字信封方式对个人信息进行加密，以保证个人信息的机密性。对于敏感个人信息,采用对敏感个人信息进行去标识化处理后再进行加密保护。可参考 GB/T 37964-2019 第 5 章去标识化过程。

——个人信息完整性保护。采用对个人信息进行签名操作的方式，保证个人信息的完整性。

——个人信息真实性保护。采用密码技术确保交互双方实体的真实性，确保个人信息数据来源的真实可靠性。

——个人信息不可否认性。用户对智能门锁操作行为和提供的个人信息的不可否认性。

5 告知和同意

为确保智能门锁系统在处理个人信息时合规，并遵循《GB/T 42574—2023 信息安全技术 个人信息处理中告知和同意的实施指南》的规定，系统需在信息收集、处理、存储、使用和删除的各环节向用户进行充分告知，并取得明确同意。从预订阶段、身份认证和访问控制阶段及信息上报阶段阐述具体的告知与用户同意实施方法和步骤。

5.1 预订阶段

5.1.1 告知的内容和方式

在预订阶段，用户需通过用于管理和操作智能门锁的软件或硬件完成个人信息的登记和授权。除参照GB/T 42574-2023第8章内容外，还需基于以下告知方式及内容，形成告知的具体实施方法和步骤。实施要点包括：

a) 首次注册使用APP时：APP在首次启动时展示《隐私政策》和《用户协议》，通过点击“同意”按钮获取用户授权；重要功能（如人脸识别）需再次单独弹窗说明，并要求明确授权；
b) 向用户告知预订时需要收集个人信息的原因及用户提供个人信息的用途，如提供用户身份认证服务；实现远程授权及开锁功能；支持数据分析及系统优化；满足法律法规要求的监管与报备需求；
c) 向用户告知预订时收集个人信息后的处理方式、保护措施等内容，如使用加密技术保护数据的机密性，防止未经授权的访问与泄露；
d) 向用户告知预订时收集个人信息后的共享规则，如在满足法律要求的前提下，说明是否与第三方共享数据及共享范围；
e) 收集的个人信息涉及敏感个人信息的，说明处理敏感个人信息的必要性，如在调用敏感权限（如摄像头、人脸识别、定位功能）时，通过系统弹窗告知用户，并说明用途；若用户拒绝授权，仅限制相关功能的使用，不影响其他功能的正常运行；
f) 收集支付账户信息(第三方支付账号、银行卡号等)时,需明确说明收集的目的、必要性、使用范围、安全保障措施和拒绝提供该信息带来的影响等。

5.1.2 同意的实施

在预订阶段，除参照GB/T 42574-2023第9章内容外，还需得到用户的同意，实施要点包括以下内容：

a) 用户进行预订时,以弹窗等形式向用户展示个人信息保护政策核心内容,同时提供完整的个人信息保护政策全文链接,并通过用户主动勾选或点击的形式取得用户同意；
b) 在为用户提供预订服务、下单支付等功能前,要求用户提供身份证号、居民身份网络可信凭证、绑定手机号码等方式以满足账号实名制的要求,并向用户告知相关的依据；
c) 用户在提供真实身份信息、敏感个人信息或预订成功进行支付时,可在网页端或APP界面提示用户了解具体的个人信息处理规则,在取得个人单独同意后才展示个人信息填写栏；
d) 提供清晰易用的隐私设置页面，允许用户随时撤回授权或注销账户。

5.2 身份认证和访问控制阶段

5.2.1 告知的内容和方式

在用户入住过程中，智能门锁和管理平台需要对用户的个人信息进行处理和身份认证并进行锁具的开启和闭合操作，除参照GB/T 42574-2023第8章内容外，还需基于以下告知方式及内容，形成告知的具体实施方法和步骤。实施要点包括：

a) 初次使用智能门锁时，在硬件界面或与APP联动的方式中，向用户明确展示收集的信息范围，如首次身份认证时需采集用户人脸、指纹等生物特征信息、身份证信息、居民身份网络可信凭证。
b) 向用户告知个人信息的处理用途，如用于本地身份认证及开锁操作；
c) 向用户告知个人信息的存储期限，当用户注销或离店后信息需告知用户及时删除或匿名化处理；
d) 向用户告知个人信息的保护措施，数据采用加密存储，并定期清理过期的无效数据。

5.2.2 同意的实施

在用户入住阶段，智能门锁和管理平台除参照GB/T 42574-2023第9章内容外，还需得到用户的同意，实施要点包括以下内容：

a) 初次使用智能门锁时，在硬件界面或与APP联动的方式中，向用户展示个人信息处理规则。用户通过APP或硬件设备确认授权后，方可完成信息收集及设备激活；

b) 敏感信息变更或注销时：系统提示用户重新确认授权，或通过APP提示完成操作；在注销账户或退房时，智能门锁自动清除本地存储的用户数据。

5.3 信息上报阶段

5.3.1 告知的内容和方式

根据有关监管要求，智能门锁管理平台需要向监管系统发送开启记录及身份信息，在此过程中，参照GB/T 42574-2023第8.2.2 提供、公开个人信息时的内容，形成告知的具体实施方法和步骤。

5.3.2 同意的实施

信息上报阶段，个人信息上报后用于维护公安安全时，需参照GB/T 42574-2023第9章同意的实施内容。

6 个人信息安全保护

6.1 智能门锁管理平台个人信息安全

智能门锁管理平台处理的个人信息包含人像信息、身份信息摘要、身份信息密文、网络标识等，其中，人像信息不能留存，其他个人信息在存储和处理的过程中按照GB/T 35273的规定执行。建议对个人信息的访问建立最小授权的访问控制策略，对安全管理人员、数据操作人员、审计人员等角色进行分离设置。

6.2 智能门锁个人信息安全

6.2.1 总则

智能门锁针对个人信息处理在取得个人同意时，严格遵照最小且必要的原则，其中使用人脸识别技术处理人像信息建议参照第5章内容取得个人的单独同意或者依法取得书面同意。

6.2.2 个人信息的收集

智能门锁对个人信息的收集按照GB/T 35273第5章中个人信息的收集规定执行，其中，包含的个人身份信息、敏感个人信息、业务信息，在收集过程中使用的安全措施包括但不限于：

a) 人像信息的安全收集：由经过安全认证的人像收集设备收集用户人脸图像，人像收集按照GB/T 35678—2017和GA/T 1723.4—2020中的要求执行，保证智能门锁收集的人像信息的可靠性与安全性；
b) 指纹信息的安全采集：在指纹信息收集过程中，指纹收集设备需要进行设备的安全认证，保证智能门锁收集的指纹信息的可靠性与安全性，指纹采集和处理过程需参见GB/T 37076—2018 第6章中的增强级要求；实名制的智能门锁中的指纹采集设备还需通过GA/T 1011-2012居民身份证指纹采集器通用技术要求；
c) 采集过程透明化：向用户明确告知人像信息的采集目的、处理方式和保护措施，并取得用户的明确同意，具体详见第5章；
d) 防未经授权采集：人像信息、指纹信息、身份信息不得通过非安全认证设备采集，确保采集方式合法合规；
e) 信息本地处理：生物特征信息等敏感个人信息在采集设备内直接处理，避免未经授权传输；
f) 采集记录可追溯：采集设备需记录数据采集日志，包括时间、操作人、采集设备信息等，确保采集行为可追溯；

g) 利用非活体数据进行认证：禁止使用静态图像、视频、简易面具等手段替代活体生物特征信息进行认证；
h) 不得采集与身份认证无直接关系的其他个人信息，如用户的健康信息、财务信息等；
i) 用户可随时撤回对信息采集的授权，系统需及时停止数据采集行为。

6.2.3 个人信息的传输

在个人信息经由专有设备收集后传输到智能门锁及管理平台等设备过程中，采用的安全措施包括但不限于：

a) 生物特征原始数据在采集后需即时加密，任何未经授权的读取、解密行为均需被阻止；
b) 专有设备收集到的生物特征原始图像不能留存或向智能门锁传输，以保障用户的个人隐私安全；
c) 对采集的指纹数据进行实时加密，防止在采集和传输过程中被窃取；
d) 个人信息在下发过程中进行加密并采用安全数据传输协议，以确保数据的机密性和完整性，禁止未经授权的访问、使用或泄露；
e) 为防止个人信息被篡改，在数据传输过程中，使用数字签名或哈希算法等方式对数据进行验证，确保数据的真实性和一致性；
f) 在向智能门锁下发个人信息之前，专有设备采用可靠的安全认证机制，确保用户完成身份认证，并确保只有被授权过的用户才能进行下发操作；
g) 在设计和实施实名制的身份认证服务时，遵守相关的法律法规，包括《个人信息保护法》等，保障用户的个人隐私和权益。

6.2.4 个人信息的存储

智能门锁对个人信息的存储时，采用的安全措施包括但不限于：

a) 个人信息存储时间遵循最小化原则，超出存储期限后，立即删除或进行匿名化处理；
b) 智能门锁在收集个人信息后，立即进行去标识化处理，将可用于恢复识别个人的信息与去标识化后的信息分开存储，并加强访问和使用的权限管理；
c) 智能门锁中的个人敏感信息进行加密存储时，仅存储个人生物识别信息的特征值数据；
d) 内置的硬件加密模块，需支持数据加密、签名和完整性验证功能，确保生物特征信息在存储过程中的机密性和完整性；
e) 存储指纹数据时使用加密技术，确保敏感信息不可逆向恢复为原始数据。

6.2.5 个人信息的使用

智能门锁对个人信息的使用包括但不限于采用以下安全措施：

a) 对智能门锁中个人信息的使用进行限制，不得超出智能门锁系统收集个人信息的目的或范围；
b) 对智能门锁中个人信息的展示进行限制，对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险；
c) 加强访问控制，确保仅在授权状态下允许解密或访问加密数据；
d) 设备内置的硬件加密模块需确保个人信息在处理和验证过程中的机密性和完整性。

6.2.6 个人信息的删除

智能门锁对个人信息的删除包括但不限于采用以下安全措施：

a) 生物特征原始数据在采集时需即时加密，任何未经授权的读取、解密行为均需被阻止；
b) 采集完成后，应及时清除采集设备中残留的原始人像图片信息，确保未授权情况下无法还原用户生物特征；
c) 在完成身份认证或使用服务后，智能门锁系统应及时清理已采集的相关身份信息。

7 其他数据安全保护

7.1 智能门锁管理平台重要数据安全

智能门锁管理平台的重要数据包含门锁标识、用户开锁信息等，这些重要数据在存储或对外传输过程中按照GB/T 39786—2021中应用和数据安全第二级及以上要求实施，同时按照GB/T 22239-2019中数据安全与存储第二级及以上规定执行。

7.2 智能门锁重要数据安全

智能门锁的重要数据包括但不限于智能门锁本身的密钥数据及用户相关的数据。

智能门锁本身的密钥数据包括但不限于智能门锁根密钥、鉴别密钥、传输保护密钥、密钥加密密钥等；用户相关的重要数据包括但不限于用户口令信息、用户权限设置信息、门锁与用户的绑定关系信息、用户专属的加密密钥信息等。

智能门锁针对重要数据具备安全保护的功能，包括但不限于采用以下安全措施：

a) 智能门锁的重要数据采用国产密码技术进行保护；
b) 智能门锁数据不能以明文形式存储和读出；
c) 智能门锁的重要数据在异常通信中断、异常断电等情况下保证数据存储的完整性，在数据使用前经过校验；
d) 删除用户后，立即从智能门锁中清除对应的用户相关重要数据；
e) 在进行实名制身份认证时，与居民身份网络认证服务系统的数据交互，在集成调用公安部身份认证的SDK完成。

7.3 智能门锁密钥管理安全

智能门锁具备密钥管理安全方面的功能，包括但不限于采用以下安全措施：

a) 智能门锁设备的密钥管理可采用对称密码体制或非对称密码体制，对称密码体制适用于智能门锁与智能门锁管理平台之间的身份鉴别、实体通信、机密性及完整性的安全保护，非对称密码体制适用于智能门锁与智能门锁管理平台之间的身份鉴别、实体通信的安全保护；
b) 智能门锁设备涉及的密钥包含但不限于智能门锁根密钥、鉴别密钥、传输保护密钥、密钥加密密钥等，智能门锁设备中的根密钥保证唯一性，即实现一机一密；
c) 智能门锁根密钥在智能门锁出厂阶段产生，传输保护密钥在智能门锁设备与智能门锁管理平台进行信息交互前临时协商产生，而智能门锁中的非对称密钥对由智能门锁、认证机构(CA)或智能门锁管理平台产生；
d) 智能门锁设备中的各类密钥信息存储于安全模块中，安全模块具备智能门锁重要数据、个人信息的安全存储、更新、删除能力，并按照GM/T 0028—2014中的安全等级二级要求执行，内置居民身份证验证安全控制模块的智能门锁在应用过程中按照GA/T 467—2019的规定执行；
e) 智能门锁设备与其他设备之间传输密钥时，采用密钥加密密钥对所传输的密钥信息进行加密，并采用国产密码技术对传输通道进行保护；
f) 当智能门锁设备中的密钥信息不再需要时，将其销毁，在销毁之后将不再有任何信息可用来恢复已销毁的密钥；
g) 当智能门锁设备中的密钥即将超过使用期限、被泄露或被怀疑不安全时，对其进行更新。

7.4 智能门锁权限数据安全

智能门锁在使用过程中对授权人和被授权人进行权限控制，保障授权可追溯。包括但不限于采用以下安全措施：

a) 智能门锁在使用过程中，用户身份认证相关数据的通信采用多种技术让用户自行选择，比如二维码、蓝牙、可见光交互，在关键领域或安防要求高的场景中，采用的交互方式需确保通信数据不容易被复制、盗取；
b) 采用最小化授权和最少特权原则，避免用户拥有超出其必要范围的访问权限，降低权限的滥用和泄露的风险；
c) 管理平台将智能门锁的访问权限分配给用户，并在权限到期后手动或自动撤销不再需要或过期的权限；
d) 管理平台通过日志记录、报表生成、告警通知等方式，对用户的权限分配和使用进行跟踪和评估，以提高权限的合规性和可信性。

7.5 设备间数据交互安全

智能门锁系统中的各设备直接及与其他设备间的交互安全，包括但不限于：
a) 智能门锁系统的设备间交互（如门锁与管理平台、手机App之间）是潜在的攻击目标，需采用硬件和协议层双重保护，确保交互数据的保密性和完整性；
b) 基于安全模块的身份认证：交互设备需内置安全模块，用于存储设备密钥和数字证书，确保通信双方身份可信。认证过程中，密钥始终在安全模块内处理，防止泄露；
c) 数据完整性校验：安全模块内实现的安全算法验证传输数据完整性，防止被篡改；
d) 异常监测与响应：结合安全模块的防篡改功能，设备可实时监测异常通信行为（如频繁访问失败），并在检测到攻击时可自毁密钥和敏感数据。

7.6 日志安全

智能门锁系统需对操作行为和设备状态进行日志记录，日志内容包括但不限于记录设备状态、用户访问、授权变更、时间戳、操作人设备ID及操作结果等。并通过安全模块确保日志的真实性和完整性，具体包括但不限于：
a) 日志存储保护：日志记录需加密存储于安全模块内，防止被恶意修改或删除；
b) 数据签名与验证：利用安全模块的数字签名功能，为日志生成签名，确保数据完整性和不可抵赖性；
c) 集中审计：管理平台需通过安全通道定期汇总各设备日志，由安全模块保护后进行集中存储和分析；
d) 异常日志告警：系统应实时监控日志内容，针对高频失败操作、异常权限变更等行为触发告警。

参 考 文 献

[1] GB/T 34978—2017 信息安全技术 移动智能终端个人信息保护技术要求

[2] GB/T 35678—2017 公共安全 人脸识别应用 图像技术要求

[3] GM/T 0036—2014 采用非接触卡的门禁系统密码应用技术指南

（本页用于出版）

中关村安信网络身份认证产业联盟团体标准

智能门锁系统个人身份认证服务

应用安全要求

T/OIDAA ×××—20××

中关村安信网络身份认证产业联盟标准化工作委员会

编　印

北京市海淀区首体南路 1 号公安部第一研究所 17 层

电话：010-68775800-8088

邮箱：ss @oidaa.cn