ICS 35.240.01
CCS L77

团　体　标　准

T/ZJAF 6—2020

智慧校园 联网型智能锁系统技术要求

Smart campus — Technical requirements for networked intelligent lock system

2020-11-18 发布　　2021-01-01 实施

浙江省安全技术防范行业协会 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。

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。

本文件由浙江省安全技术防范行业协会提出并归口。

本文件起草单位：掌门物联科技（杭州）股份有限公司、浙江正元智慧科技股份有限公司、嘉兴市南湖区保安服务有限公司、广东必达保安系统有限公司、杭州尚量标准化管理技术咨询有限公司、杭州惟远信息技术有限公司、浙江中浩应用工程技术设计院有限公司、杭州英杰电子有限公司、浙江省安全技术防范行业协会。

本文件主要起草人：许哲昌、蔡宇峰、徐敏、陈伟禧、俞超峰、张聚杰、葛良建、黄柳、邱宇芃、文庆、胡笑、龚丹丹。

智慧校园 联网型智能锁系统技术要求

1 范围

本文件规定了智慧校园联网型智能锁系统的系统架构、功能要求、性能要求、信息安全要求和运维要求。

本文件适用于校园场所使用的联网型智能锁系统的总体规划、方案设计、工程建设、运行维护以及与之相关的设备研发、生产和质量控制，其他场所也可参考使用。

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 36342—2018 智慧校园总体框架

GB/T 36920—2018 锁具 术语

GA 374—2019 电子防盗锁

3 术语和定义

GB/T 36920、GA 374界定的术语和定义适用于本文件。

4 系统架构

4.1 智慧校园联网型智能锁系统（以下简称“系统”）是智慧校园信息系统的组成部分。系统以联网型智能锁（以下简称“智能锁”）为终端工具，采用物联通信技术，实现对智能锁的远程智能化管理，并对校园安全、学生行为进行辅助管理。

4.2 系统由智能锁、通信协议和智能锁管理平台（以下简称“管理平台”）组成，系统架构如图 1 所示。

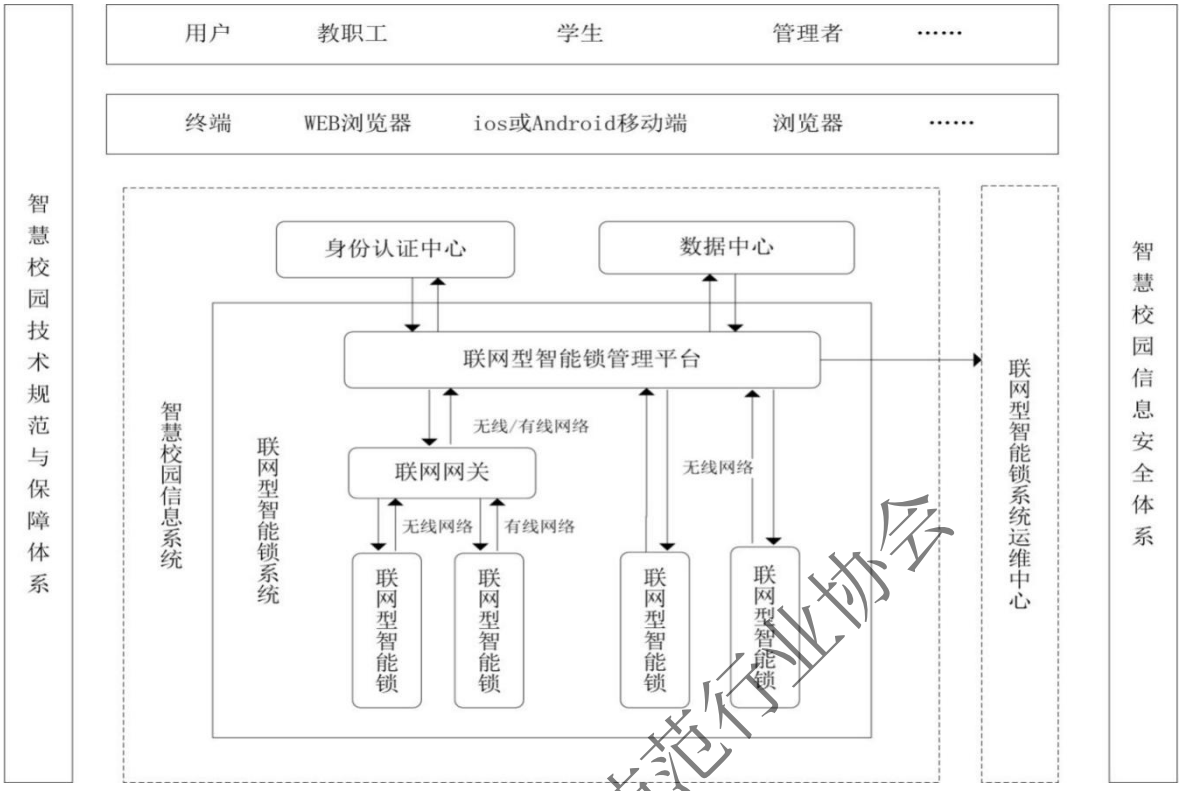

图 1 智慧校园联网型智能锁系统架构图

4.3 通过身份认证中心认证鉴权后，教职工、学生、管理者等用户可通过 WEB 浏览器、iOS 或 Android 移动端、浏览器等访问系统，以获取资源和服务。

4.4 数据中心向系统提供校园基础数据，接收系统产生的管理数据并予以保存。

4.5 管理平台采用有线或无线通信方式通过联网网关管理智能锁，或采用无线通信方式直接管理智能锁。

4.6 系统可向运维中心提供系统服务器运行状态、智能锁运行状态系统等数据。

4.7 智慧校园信息系统未建身份认证中心、数据中心或运维中心时，系统应支持相应的功能。

5 功能要求

5.1 智能锁

5.1.1 基本功能

应符合GA 374—2019中5.3的规定。

5.1.2 通信接口

5.1.2.1 可支持 Wi-Fi、Bluetooth、ZigBee、LoRa、NB-Iot 等通信协议或智慧校园专用通信协议。

5.1.2.2 宜支持多种通信方式进行复合组网。

5.1.3 系统升级

应支持远程升级和串口本地升级。

5.1.4 数据存储

管理平台出现故障或网络中断时，应支持循环存储脱机数据，并在故障修复后上传所存储的事件记录和报警信息。

5.1.5 启闭管理

5.1.5.1 在断电、断网等情况下，应支持正常开启和锁闭。

5.1.5.2 应支持密码、射频卡、指纹、人脸等两种或两种以上的开启方式。

5.2 联网网关

5.2.1 系统升级

5.2.1.1 应支持远程升级和串口本地升级。

5.2.1.2 应支持管理平台对智能锁的远程升级。

5.2.2 数据恢复

管理平台出现故障或网络中断时，应支持存储智能锁状态数据和行为数据，并在故障修复后上传所存储的数据。

5.3 管理平台

5.3.1 系统管理

5.3.1.1 应支持用户信息的批量操作。

5.3.1.2 应支持电子钥匙授权信息的批量导入和分配。

5.3.1.3 应支持对智能锁软件、系统软件进行升级。

5.3.1.4 应支持本地数据库进行手动或自动备份，备份信息包括但不限于：

——部门信息：部门名称、部门编号；

——教职工信息：工号、姓名、性别、所属部门；

——学生信息：学号、姓名、性别、所属班级、所属院系；

——电子钥匙信息：钥匙 ID、所属人员、钥匙状态、钥匙有效期。

5.3.1.5 宜支持用户、钥匙信息与数据中心的数据自动同步。

5.3.2 权限管理

5.3.2.1 应支持权限信息的批量操作。

5.3.2.2 应支持设置开锁权限的生效时间和失效时间。

5.3.2.3 应支持预授权和实时授权的开锁授权方式。

5.3.2.4 宜支持由智慧校园系统第三方平台管理开锁授权、远程开锁等功能。

5.3.3 终端管理

5.3.3.1 应支持对智能锁运行状态的监测和查询功能。

5.3.3.2 宜支持对智能锁运行信息的数据挖掘功能。

5.3.4 故障管理

5.3.4.1 应支持智能锁的故障告警功能。

5.3.4.2 宜支持人工设置和调整故障信息告警的阀值。

5.3.5 日志管理

5.3.5.1 应记录操作日志，包括但不限于用户名、电子钥匙 ID 授权信息、操作时间、操作动作、操作对象、操作结果等信息。
5.3.5.2 应支持日志查询、日志输出和历史告警查询功能。

5.3.6 数据管理

5.3.6.1 应支持与身份认证中心、数据中心或第三方管理软件/系统的数据与功能对接。
5.3.6.2 应支持智能锁启闭、异常告警、电池电量、运维等数据与数据中心及运维中心数据的交互功能。
5.3.6.3 开门记录应保存不少于 6 个月，报警记录和操作记录应保存不少于 12 个月，并同步到数据中心。
5.3.6.4 宜由校园身份认证中心作为用户身份认证鉴权的主入口。

5.4 运维中心

5.4.1 宜部署在智慧校园信息系统上，对系统运行状态进行监控。
5.4.2 部署在公有云时，系统宜采用单向传输方式向运维中心提供运维数据。

6 性能要求

6.1 智能锁应符合 GA 374 的规定。
6.2 智能锁电池容量应保证锁体连续正常启、闭 8000 次以上。
6.3 在不依赖于第三方的情况下，管理平台及所采用的通信技术应支持大于 10000 把智能锁联网。
6.4 在权限已下发状态下，采用刷卡、指纹等方式的开锁响应时间不应大于 0.8s。
6.5 在设备联机状态下，通过网络即时开门成功率不应低于 95%，响应时间不应大于 5s。
6.6 在设备联机状态下，批量授权 10 条/锁耗时不应大于 10s。
6.7 在断网情况下，应支持循环存储脱机数据不低于 100 条。
6.8 智能锁牢固度宜不低于 30 万次启闭。

7 信息安全要求

7.1 应符合 GB/T 36342—2018 第 10 章的规定。
7.2 管理平台与联网网关、联网型智能锁之间的数据传输应采用加密算法。
7.3 应定期对管理平台进行软件漏洞修复或系统更新。

8 运维要求

8.1 运维中心应提供 7x24h 服务响应，软件问题应在 48h 内提供解决方案或临时替代方案，硬件问题若需更换设备或上门服务的，按国家有关三包规定或双方合同约定执行。
8.2 宜对智能锁电池进行定期更换。
8.3 宜对智能锁进行不定期固件升级和漏洞修复。