ICS 35.240.15
CCS L 64

中华人民共和国国家标准

GB/T 44402.1—2024

卡及身份识别安全设备 数字钥匙系统 第1部分：参考架构

Card and identification security devices—Digital key system—Part 1:Reference architecture

2024-08-23 发布　　2025-03-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件是GB/T 44402《卡及身份识别安全设备　数字钥匙系统》的第1部分。GB/T 44402已经发布了以下部分：

——第1部分：参考架构。

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。

本文件由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、江苏赛西科技发展有限公司、蚂蚁科技集团股份有限公司、中山市澳多电子科技有限公司、深圳市和讯华谷信息技术有限公司、北京交通大学、北京安御道合科技有限公司、东信和平科技股份有限公司、北京握奇数据股份有限公司、上海银基信息安全技术股份有限公司、紫光同芯微电子有限公司、联想中天科技有限公司、中国汽车工程研究院股份有限公司、北京眼神科技有限公司、北京雅光谷信息系统有限公司、清研智行（北京）科技有限公司、北京科技大学、金邦达有限公司、国民技术股份有限公司、本田技研工业（中国）投资有限公司、北京中电华大电子设计有限责任公司、东莞市翰普电子科技有限公司、新大陆数字技术股份有限公司、楚天龙股份有限公司、上海复旦微电子集团股份有限公司、武汉天喻信息产业股份有限公司、中国邮电器材集团有限公司、罗克佳华科技集团股份有限公司、西安凯虹电子科技有限公司、北京华大智宝电子系统有限公司、矩网科技有限公司、无锡盈达聚力科技有限公司、斯科智能五金（绍兴）有限公司、北京远景视点科技有限公司、深圳市小麦飞扬科技有限公司、布洛克（北京）数据科技有限公司、星汉智能科技股份有限公司、中移互联网有限公司、联友智连科技有限公司、深圳市艾克瑞电气有限公司、徐州国云信息科技有限公司、深圳市昇润科技有限公司、深圳赛西科技有限公司。

本文件主要起草人：张璋、王文峰、高睿鹏、张晖、林冠辰、冯锋、陈光炎、赵峻莉、宋继伟、耿力、高健、曹国顺、王永涛、丁程龙、邢薇薇、刘吉强、钟陈、白婧、蒋小辉、赵轶、周游、兰瑞芬、李扬、吕雪、杨春林、袁永贵、裘有斌、王曲、徐木平、杨贤伟、胡乾、陈峰、李霖、张劲松、黄海明、苏昆、钱涛、李玮、胥建民、韩劭之、宋博见、柴宇佳、孙春桂、甘戈、王冬生、陆惠良、于洪方、高路、罗娅、曹晓青、庄仁峰、赖燕燕、文军红、史臣、孟庆森、范指江、陈炽华、何智勇。

引　言

随着云计算、大数据、物联网及人工智能等新一代信息技术的高质量发展，我国数字经济发展已进入新的阶段，传统的钥匙技术也从原来的金属钥匙发展到现在存储于卡、手机、手表等不同形式载体上的数字钥匙，采用信息技术的数字钥匙取代传统钥匙将是发展趋势。数字钥匙具有以下优势：一是时空限制小，打破传统钥匙的时空限制，用户可以随时随地使用；二是方便使用，对发行方来说发钥匙更方便、便捷，用户可根据情况对钥匙进行设置；三是更专业和安全，根据用户的身份重新构建钥匙的权限。数字钥匙不是一个可以独立使用的实体，其应用通过数字钥匙系统来实现。数字钥匙系统主要包括主用户/从用户终端、电子锁终端、管理服务器等。数字钥匙的应用涉及车钥匙、房屋门锁钥匙、柜子钥匙等多个民生相关场景，极大地方便了人们的日常生活。GB/T 44402《卡及身份识别安全设备 数字钥匙系统》旨在规定数字钥匙系统的参考架构、通用规范、数据对象与编码规则、终端与锁具传输层协议及测试方法、应用层协议及测试方法,拟由五个部分构成。

——第1部分：参考架构。目的在于确立数字钥匙系统的功能框架和业务流程。

——第2部分：通用规范。目的在于规定数字钥匙系统的分类代码、功能、性能、安全等相关要求以及对应的测试方法。

——第3部分：数据对象与编码规则。目的在于规定数字钥匙系统数据的编码规则与通用格式。

——第4部分：终端与锁具传输层协议。目的在于规定数字钥匙终端与锁具的传输层协议。

——第5部分：应用层协议。目的在于规定数字钥匙系统的应用层协议。

卡及身份识别安全设备
数字钥匙系统　第1部分：参考架构

1　范围

本文件确立了数字钥匙系统的功能架构和业务流程。

本文件适用于数字钥匙系统的研发、设计以及应用。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

数字钥匙　digital key

用于控制电子锁终端（3.4）启闭的一种数字化凭证。

注：用户使用凭证进行访问权限鉴别。

3.2

数字钥匙系统　digital key system

由用户终端（3.3）、电子锁终端（3.4）、管理服务器等组成，对数字钥匙生存周期进行管理的软硬件实体。

3.3

用户终端　user terminal

能够基于短距离通信模块实现对电子锁终端（3.4）的访问与控制，并承载数字钥匙（3.1）的硬件实体。

注：短距离通信模块包括近场通信（NFC）、低功耗蓝牙（BLE）、超宽带（UWB）、星闪等通信模块。

3.4

电子锁终端　electronic lock terminal

对数字钥匙进行鉴别，并控制机械执行机构完成启闭的电子锁具装置。

3.5

属性　attribute

实体（3.8）的特征或特性。

[来源：ISO/IEC 24760－1:2019，3.1.3]

3.6

鉴别　identification

为实体（3.8）的身份（3.9）的合法性提供保证。

[来源：ISO/IEC 29115:2013，3.2，有修改]