ICS 35.240.15
CCS L 64

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44402.1-2024

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

卡及身份识别安全设备 数字钥匙系统 第1部分：参考架构

Issued on: August 23, 2024 **Implemented on: March 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting is required.

This document is part 1 of GB/T 44402 "Card and identity security device digital key system". GB/T 44402 has been The following parts were published.

Part 1: Reference Architecture. - Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document was proposed and coordinated by the National Technical Committee for Information Technology Standardization (SAC/TC 28).

This document was drafted by: China Electronics Technology Standardization Institute, Jiangsu CESI Technology Development Co., Ltd., Ant Technology Group Co., Ltd.

Co., Ltd., Zhongshan Aoduo Electronic Technology Co., Ltd., Shenzhen Hexun Huagu Information Technology Co., Ltd., Beijing Jiaotong University, Beijing Anyu Daohe Technology Co., Ltd., Eastcompeace Technology Co., Ltd., Beijing Watchdata Co., Ltd., Shanghai Yinji Information Security Technology Co., Ltd.

Co., Ltd., Unigroup Tongxin Microelectronics Co., Ltd., Lenovo Zhongtian Technology Co., Ltd., China Automotive Engineering Research Institute Co., Ltd.

Beijing Yanshen Technology Co., Ltd., Beijing Yaguanggu Information System Co., Ltd., Tsinghua Zhixing (Beijing) Technology Co., Ltd., Beijing Science and Technology Co., Ltd.

University of Science and Technology, Goldpac Co., Ltd., National Technology Co., Ltd., Honda Motor (China) Investment Co., Ltd., Beijing Zhongdian Hua Da Electronic Design Co., Ltd., Dongguan Hanpu Electronic Technology Co., Ltd., Newland Digital Technology Co., Ltd., Chutianlong Shares Co., Ltd., Shanghai Fudan Microelectronics Group Co., Ltd., Wuhan Tianyu Information Industry Co., Ltd., China Post and Telecommunications Equipment Group Co., Ltd.

Ltd., Rockwell Automation Technology Group Co., Ltd., Xi'an Kaihong Electronic Technology Co., Ltd., Beijing Huada Zhibao Electronic System Co., Ltd.

Company, Juwang Technology Co., Ltd., Wuxi Yingda Juli Technology Co., Ltd., Sike Intelligent Hardware (Shaoxing) Co., Ltd., Beijing Yuanjing Viewpoint Technology Co., Ltd., Shenzhen Xiaomai Feiyang Technology Co., Ltd., Block (Beijing) Data Technology Co., Ltd., Xinghan Intelligent Technology Co., Ltd.

Co., Ltd., China Mobile Internet Co., Ltd., Lianyou Zhilian Technology Co., Ltd., Shenzhen Aikerui Electric Co., Ltd., Xuzhou Guoyun Information Technology Co., Ltd., Shenzhen Shengrun Technology Co., Ltd., and Shenzhen CESI Technology Co., Ltd.

The main drafters of this document are: Zhang Zhang, Wang Wenfeng, Gao Ruipeng, Zhang Hui, Lin Guanchen, Feng Feng, Chen Guangyan, Zhao Junli, Song Jiwei, Geng Li, Gao Jian, Cao Guoshun, Wang Yongtao, Ding Chenglong, Xing Weiwei, Liu Jiqiang, Zhong Chen, Bai Jing, Jiang Xiaohui, Zhao Yi, Zhou You, Lan Ruifen, Li Yang, Lü Xue, Yang Chunlin, Yuan Yonggui, Qiu Youbin, Wang Qu, Xu Muping, Yang Xianwei, Hu Qian, Chen Feng, Li Lin, Zhang Jinsong, Huang Haiming, Su Kun, Qian Tao, Li Wei, Xu Jianmin, Han Mizhi, Song Boyan, Chai Yujia, Sun Chungui, Gang Ge, Wang Dongsheng, Lu Huiliang, Yu Hongfang, Gao Lu, Luo Ya, Cao Xiaoqing, Zhuang Renfeng, Lai Yanyan, Wen Junhong, Shi Chen, Meng Qingsen, Fan Zhijiang, Chen Chihua, He Zhiyong.

Introduction

With the high-quality development of new-generation information technologies such as

cloud computing, big data, the Internet of Things, and artificial intelligence, China's digital economy has made great progress.

Entering a new stage, traditional key technology has also evolved from the original metal key to the current storage on different forms of carriers such as cards, mobile phones, watches, etc.

Digital keys, using information technology to replace traditional keys will be a development trend. Digital keys have the following advantages. First, time and space The restrictions are small, breaking the time and space restrictions of traditional keys, and users can use them anytime and anywhere; secondly, it is easy to use, and it is more convenient for the issuer to issue keys.

It is convenient and easy to use. Users can set the key according to the situation. Third, it is more professional and safe. The key authority is rebuilt according to the user's identity.

The digital key is not an entity that can be used independently, and its application is realized through the digital key system. The digital key system mainly includes Master/slave user terminals, electronic lock terminals, management servers, etc. The application of digital keys involves car keys, house door lock keys, cabinet keys, etc.

GB/T 44402 Cards and identity recognition security devices - Digital The Digital Key System aims to define the reference architecture, general specifications, data objects and encoding rules, and terminal and lock transport layer protocols of the digital key system.

It is planned to consist of five parts. protocol and test method, application layer protocol and test method.

Part 1: Reference Architecture. The purpose is to establish the functional framework and business processes of the digital key system.

Part 2: General Specifications. The purpose is to specify the classification code, function, performance, security and other related requirements of the digital key system and the corresponding test methods.

Part 3: Data objects and encoding rules. The purpose is to specify the encoding rules and common format of digital key system data.

Part 4: Terminal and lock transport layer protocol. The purpose is to specify the transport layer protocol between digital key terminals and locks. - Part 5: Application layer protocol. The purpose is to specify the application layer protocol of the digital key system. - Cards and identity security devices Digital Key System Part 1: Reference Architecture

1 Scope

This document establishes the functional architecture and business processes of the digital key system.

This document applies to the research and development, design and application of digital key systems.

2 Normative references

This document has no normative references.

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 digital key

A digital certificate used to control the opening and closing of the electronic lock terminal (3.4).

Note. Users use credentials to authenticate access rights.

3.2 Digital key systemdigital key system

It consists of a user terminal (3.3), an electronic lock terminal (3.4), a management server, etc., and is a software that manages the life cycle of digital keys. Hardware entity.

3.3 User terminal

Able to access and control the electronic lock terminal (3.4) based on the short-range communication module and carry the hardware of the digital key (3.1) entity.

Note. Short-range communication modules include near field communication (NFC), low-power Bluetooth (BLE), ultra-wideband (UWB), and Star Flash communication modules.

3.4 Electronic lock terminal

An electronic lock device that authenticates the digital key and controls the mechanical actuator to open and close.

3.5 attribute

Characteristics or properties of an entity (3.8) [Source. ISO /IEC 24760-1 2019, 3.1.3]

3.6 Identification

Provide assurance of the legitimacy of the identity (3.9) of an entity (3.8).

[Source. ISO /IEC 29115 2013, 3.2, with modifications]