

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 44602-2024

**Cybersecurity technology - Cybersecurity technical
specification for smart lock products**

网络安全技术 智能门锁网络安全技术规范

Issued on: September 29, 2024

Implemented on: April 1, 2025

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

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Abbreviations	2
5 Overview	2
6 Smart door lock security technical requirements	3
6.1 Smart door lock terminal security technical requirements	3
6.2 Security Technical Requirements for Smart Door Lock Access Gateway	6
6.3 Security Technical Requirements for Smart Door Lock Management Platform	7
6.4 Security technical requirements for smart door lock control terminal	10
6.5 Security requirements	12
7 Smart door lock security evaluation method	14
7.1 Smart Door Lock Terminal Security Evaluation Method	14
7.2 Security Evaluation Method for Smart Door Lock Access Gateway	20
7.3 Security Assessment Methods for Smart Door Lock Management Platform	23
7.4 Smart door lock control terminal security evaluation method	27
7.5 Security Assessment Methods	32
39 References	42

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. 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 Cybersecurity Standardization Technical Committee (SAC/TC260). This document was drafted by: The Third Research Institute of the Ministry of Public Security, China Cybersecurity Review and Certification and Market Supervision Big Data Center, National Computer Network and Information Security Management Center, Qingdao Haier Smart Home Appliance Technology Co., Ltd., Institute of Software, Chinese Academy of Sciences, Hangzhou EZVIZ Software Co., Ltd. Ltd., Zhejiang Dahua Technology Co., Ltd., Zhongshan Lock Industry Association, China Mobile

Communications Group Co., Ltd., China Telecom Group Co., Ltd. Company, National Information Center, First Institute of Telecommunications Science and Technology Co., Ltd., Alibaba (Beijing) Software Services Co., Ltd., Shenzhen Kai Deshi Intelligent Technology Co., Ltd., Zhejiang Deshiman Technology Intelligence Co., Ltd., Shanghai Jiaweisi Information Technology Co., Ltd., Luke Technology (Beijing) Co., Ltd., Shuobo Information Technology (Shanghai) Co., Ltd., Zhejiang Zhibei Information Technology Co., Ltd., Shanghai Wudun Information Technology Co., Ltd., Yidun (Shanghai) Intelligent Technology Co., Ltd., Yikang Intelligent Technology (Shanghai) Co., Ltd., Dongwu Shian IoT Technology (Jiangsu) Co., Ltd., Information Engineering Institute of the Chinese Academy of Sciences, Huawei Terminal Co., Ltd., China Mobile (Hangzhou) Information Technology Co., Ltd., Qingdao Guochuang Intelligent Home Appliances Research Institute Co., Ltd., Ningbo Zhenhai Shenzhou Locks Co., Ltd., State Grid Zhejiang Electric Power Co., Ltd. Power Science Research Institute, Inner Mongolia Digital Economy Security Technology Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd., Beijing Bangbang Security Technology Co., Ltd. Company, Beijing Zhiyou Network Security Technology Co., Ltd., Shanghai Sidun Information Technology Co., Ltd., Guangdong Sakura Intelligent Technology Co., Ltd., Zhongshan Yang Ge Lock Industry Co., Ltd. and Zhongshan Mingguang Intelligent Technology Co., Ltd. The main drafters of this document are. Liu Jishun, Lu Zhen, Shen Liang, Zhang Yan, Li Haipeng, Sun Yongqing, Hu Jinming, Zhang Zhiqiang, Shen Yongbo, He Qinglin, Li Li, Yang Chen, Yan Min, Li Wei, Yu Xiaojie, Feng Xiuying, Jiang Weiqiang, Wang Lei, Wang Laifu, Chen Yuehua, Gao Jinjun, Fang Qiang, Su Qiyun, Dong Qiguang, Shu Shouheng, Xiang Yang, Li Zhiwei, Zhou Zhengda, Xu Mengyu, Zhu Yixiang, Zhu Pengcheng, Min Hao, Li Fenghua, Chen Zhiyuan, Lu Xiaoming, Wang Kai, Wu Qiliang, Sun Xin, Cai Yuyuan, Zhou Yachao, Lu Zuohua, Cheng Zhili, Zeng Songfeng, Wang Haiqiang, Zhou Lixin, Jin Ze. Network security technology Intelligent door lock network security technical specifications

1 Scope

GB/T 44602-2024 is the Chinese cybersecurity specification for smart lock products. A smart lock is the rare consumer device where a software vulnerability opens a physical door, and the Chinese market has more of them than any other; the document treats the product as the four-part system it really is rather than as a lock, and secures each part. It gives the composition of the smart lock system and then sets the security technical requirements for the lock terminal itself, for the access gateway, for the management platform and for the control end, that is the phone application or panel, together with the security assurance requirements drawn from GB/T 18336. It then describes, at equal length, the assessment method for every one of those requirements, so that the document can be used directly as a test specification, and it divides the results into security levels. An informative annex analyses the common security risks of smart locks, and a normative annex gives the minimum set of requirements and assessment methods for the basic level

and for the enhanced level. It applies to the design, development, testing and evaluation of smart lock cybersecurity, which makes it the governing text for any manufacturer, platform operator or test laboratory in this market.

This document gives the structure of the smart door lock and specifies the network security of the smart door lock terminal, access gateway, management platform, and control terminal. Technical requirements and security level classification are described, and corresponding evaluation methods are described. This document applies to the cybersecurity design, development, testing and evaluation of smart door locks.

2 Normative references

The contents of the following documents constitute essential clauses of this document through normative references in this document. For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document.

GB/T 18336.1-2024 Cybersecurity technology Information technology security assessment criteria Part

3 Terms and definitions

GB/T 18336.1-2024, GB/T 18336.3-2024, GB/T 25069, GB/T 33745-2017, GB/T 35273-
For the purposes of this document, the following terms and definitions are applicable.

3.1 Smart door locks Use biometrics, electronic tags, wireless remote control codes, electronic passwords or remote control commands as authentication credentials to control the door lock to open or close. Close, the door lock system consists of a door lock terminal, an access gateway, a management platform and a control terminal.

3.2 mutual authentication An entity authentication mechanism where both entities provide identity assurance information to each other. [Source: GB/T 15843.1-2017, 3.18].

3.3 IC card A card with an integrated circuit chip embedded inside.

Note. The CPU card is an IC card containing a central processing unit (CPU).

3.4 sensitive information Information that may have a serious impact or damage to users if leaked, modified, destroyed or lost.

Note. Sensitive information includes but is not limited to keypad passwords, Bluetooth keys, user personal identification numbers (PINs), user IDs, smart card authentication data, user biometrics, Feature information, device root key and other information.