

ICS 35.240.15
CCS L70



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

GB/T 44901.1-2024

**Cards and security devices for personal identification - Chip
operating system - Part 1: General requirements**

卡及身份识别安全设备 片上操作系统 第1部分：总体要求

Issued on: October 26, 2024

Implemented on: May 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 System Architecture	2
6 Functional Requirements	5
6.1 Basic Layer	5
6.2 Application Support Layer	7
6.3 Application Interface Layer	8
7 Performance Requirements	11
7.1 Time Characteristics	11
7.2 Resource Utilization	12
7.3 Capacity	12
7.5 Usability	12
7.6 Reliability	13
8 Safety Requirements	13
8.1 Random Number Generator	13
8.2 Cryptographic Operations	13
8.3 Security Features	13
8.4 Permission Management	13

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. This document is Part 1 of GB/T 44901 "Operating Systems on Chips for Cards and Identity Security Devices". The following parts were published.

1. General requirements. 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/TC28). This document was drafted by: China Electronics Standardization Institute, Beijing Zhixin

Microelectronics Technology Co., Ltd., Jiangsu CESI Technology Development Co., Ltd., Shenzhen Chuangzi Technology Co., Ltd., Jiangsu Yiyuan Technology Co., Ltd., Shenzhen CESI Information Technology Co., Ltd., Eastcompeace Technology Technology Co., Ltd., Beijing Watchdata Co., Ltd., Wuhan Tianyu Information Industry Co., Ltd., Feitian Chengxin Technology Co., Ltd. Co., Ltd., Beijing China Electronics Huada Electronic Design Co., Ltd., Goldbond Co., Ltd., Beijing Anyudaohe Technology Co., Ltd., China Mobile Financial Rong Technology Co., Ltd., Beijing Huada Zhibao Electronic Systems Co., Ltd., Beijing Huahong Integrated Circuit Design Co., Ltd., Newland Digital Technology Co., Ltd., China Railway 19th Bureau Group Co., Ltd., China UnionPay Co., Ltd., Unisplendour Tongxin Microelectronics Co., Ltd., Datang Microelectronics Technology Co., Ltd., Shanghai Fudan Microelectronics Group Co., Ltd., Sichuan Shangtou Information Technology Co., Ltd., Zhongguancun Xinhai Zeyou Technology Co., Ltd., Chutianlong Co., Ltd., Shanghai Mite Printing Co., Ltd., Shenzhen HiSilicon Semiconductor Co., Ltd., United Network Communications Group Co., Ltd. The main drafters of this document are. Cao Guoshun, Xu Jing, Lei Yun, Jiang Riyong, Xu Muping, Huang Xiaopeng, Zhao Yi, Gao Jian, Cai Chunshui, Su Kun, Zhu Pengfei, Li Yan, Liu Hongmei, Xie Yifu, Han Mozhi, Sun Jian, Zhang Lei, Sun Chungui, Guo Yanhong, Guan Zhenxiang, Han Bo, He Jun, Zhang Shuliang, Xu Wenjun, Li Yang, Sun Jingang, Huang Haiming, Shu Min, Bai Jing, Ma Yiming, Fu Qingqin, Cao Haitao, Song Yiting, and Wang Haitao.

On-chip operating system refers to the operating system running on the security chip of the card and identity identification security device, which is usually used in smart cards, US-BKEY, ESAM, SE and other products. In order to establish a unified card and identity security device on-chip operating system architecture, standardize the unified Application format and application interface, improve the interoperability between peripheral devices and security chips, provide a basis for testing and verification, and formulate GB/T 44901 "On-chip operating systems for cards and identity recognition security devices". GB/T 44901 "On-chip operating systems for cards and identity authentication devices" aims to ensure the availability and security of on-chip operating systems. It is convenient for interconnection, intercommunication and compatibility between systems and devices, and is conducive to standardizing different types of products and dividing the on-chip operating system according to function and level. The design and development of the on-chip operating system for guidance cards and identity recognition security devices is planned to consist of six parts.

1.General requirements. The purpose is to establish the architecture and system composition of the on-chip operating system and to provide a series of specifications for the on-chip operating system. Provides guidelines and indexes, and standardizes the overall functionality, performance, security, compatibility, usability and other software quality characteristics of the on-chip operating system. Sexual requirements.

2.General base layer technical requirements. The purpose is to standardize the specific functional technologies of the general base layer of the on-chip operating system Require.

3. Technical requirements for the base layer supporting post-application download. The purpose is to standardize the application of the base layer supporting post-application download. Specific functional technical requirements for installers and actuators.

4. Technical requirements for the application support layer. The purpose is to standardize the application management, life cycle management and application support layer Specific functional technical requirements for global services.

5. Technical requirements for the application interface layer. The purpose is to standardize the data communication, storage management, file system, and other aspects of the on-chip operating system. System application programming interface.

6. Security technical requirements. The purpose is to standardize the information security protection objectives and information security functions of the on-chip operating system Technical requirements. This document standardizes the overall technical requirements for on-chip operating systems for cards and identity security devices, and provides It is the basis for design, development and testing, which facilitates users to use the on-chip operating system, improves the interoperability between industries and devices, and better Promote communication and technical cooperation within the card and identity recognition security equipment industry chain. On-chip operating system for cards and identity security devices Part

1 Scope

GB/T 44901.1-2024 is Part 1 of the Chinese series on the chip operating system of cards and personal identification security devices. A COS is the software inside a smart card, a SIM, an eID or a security key, and it is written under constraints almost nothing else shares: a few tens of kilobytes of memory, no reliable power, an adversary who physically holds the device and can cut its supply mid-write, and a requirement that the keys never leave. Part 1 sets the general requirements. It defines the system architecture and then the functional requirements at the basic layer, the application support layer and the application interface layer, the performance requirements covering timing characteristics, resource utilisation, capacity and reliability, and the security requirements, including the random number generator, the cryptographic operations, the key management, the access control and the protection against physical and side channel attack. It takes effect on 1 May 2025.

This document specifies the system architecture, functional requirements, performance requirements, and security requirements of the on-chip operating system. This document applies to the research and development, testing, acceptance and application of on-chip operating systems for cards and identity recognition security devices.

2 Normative references

This document has no normative references.

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1 security chip security chip An integrated circuit chip that contains cryptographic algorithms, security functions, and can implement a key management mechanism. [Source: GM/T 0008-2012, 3.1.3]

3.2 chip operating system An operating system that runs on the security chip in cards and identity security devices.

Note. Usually used in smart cards, USBKEY, ESAM, SE and other product forms.

3.3 application Data structures, data elements and program modules required to meet specific functions. [Source: GB/T 16649.4-2010, 3.3]

3.4 loadablefile A specific file generated by the application compiler that can be loaded into the on-chip operating system.

3.5 executable file A file generated by the application installer and capable of being executed by the on-chip operating system.

3.6 executable module executablemodule The executable code for a single application is contained in an executable file.

Note. If the executable file contains this module, it will be installed, otherwise it will not be installed.

3.7 Atomic operation atomicoperation A single operation unit in which all data operations on the nonvolatile storage area involved are successful or remain in their original state.