

ICS 35.240.15

CCS L 71



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

GB/T 45498.3-2025

**Specifications for the social security card one-card-pass of the
People's Republic of China - Part 3: Security specifications**

中华人民共和国社会保障卡一卡通规范 第3部分：安全规范

Issued on: March 28, 2025

Implemented on: March 28, 2025

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

Table of Contents

Preface	III
Introduction	IV
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Abbreviations	2
5 Security Architecture	3
6 Carrier safety requirements	3
6.1 Physical Social Security Card Security	3
6.2 Electronic Social Security Card Security	5
7 Terminal Security Requirements	6
7.1 General	6
7.2 Terminal security management requirements	6
7.3 Terminal security technical requirements	7
8 Platform Security Requirements	8
8.1 General	8
8.2 Management requirements	8
8.3 Technical requirements	10
9 Data security requirements13	13
9.1 General	13
9.2 Basic Data Security	13
9.3 Card Service Data Security	16
9.4 Application Data Security	18
10 Key security requirements	20
10.1 General	20
10.2 Key management requirements	20
10.3 Social Security PSAM Card Management	20
10.4 Hardware Key Device Security	21
10.5 Social Security Card Key Management System Security	21
10.6 Card Carrier Key Security	21
10.7 Terminal Key Security	22

Appendix A (Normative) Calculation method for physical social security card security message	23
A.1 8-byte block cipher algorithm MAC calculation	23
A.2 16-byte block cipher algorithm MAC calculation	23
A.3 Process key calculation method	23
A.4 Calculation of identification data	24
A.5 Data encryption calculation method	24
A.6 Data decryption calculation method	24
A.7 Social Security Card Key	25
Appendix B (Normative) Security Technical Requirements for Access to Electronic Social Security Card Service Channels	28
B.1 Overview	28
B.2 Basic functional safety	28
B.3 System Security	29
B.4 Authentication Security	30
B.5 Data Security31 B.6 Communication Security	31
B.7 Cryptographic Algorithm Security	31
B.8 Interface Security	32
B.9 Key Management	32
B.10 Business Process Environment Management	33
B.11 Electronic Social Security Card Service Channel Software Management	33
Appendix C (Normative) Requirements for data transfer of social security card asymmetric authentication application card making	34
C.1 Overview	34
C.2 Technical requirements	34
C.3 Interface Specifications	34
Reference	40

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 3 of GB/T 45498 "Specifications for the Social Security Card of the People's Republic of China".

The following parts were published.

- Part 1: Basic specifications;
- Part 2: Application specifications;
- Part 3: Safety regulations;
- Part 4: Terminal specifications.

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 is proposed and coordinated by the Ministry of Human Resources and Social Security of the People's Republic of China.

This document was drafted by: Information Center of the Ministry of Human Resources and Social Security, the People's Bank of China, Jinbaoxin Social Security Card Technology Co., Ltd., Beijing Weiwang Technology Development Co., Ltd., Beijing Guoxin Bofei Technology Development Co., Ltd., China Electronics Technology Network Security Technology Co., Ltd., Tianjin Social Insurance Fund Management Center, Liaoning Social Insurance Service Center, Fujian Human Resources and Social Security Information Center, Hubei Human Resources and Social Security Information Center, Guizhou Human Resources and Social Security Information Center, Shaanxi Human Resources and Social Security Information Center According to the Cyber Security Supervision Center, Ningxia Hui Autonomous Region Social Insurance Administration, China National Institute of Standardization, China Electronics Technology Standard Institute of Chemistry, Beijing CEC Huada Electronic Design Co., Ltd., Puhua Chengxin Information Technology Co., Ltd., China Electronics Technology Group Corporation The 15th Research Institute, Sanwei Xinan Technology Co., Ltd., Datang Microelectronics Technology Co., Ltd., Tsinghua Unigroup Tongxin Microelectronics Co., Ltd., Shanghai Fudan Microelectronics Group Co., Ltd., Shenzhen Deka Technology Co., Ltd., Shenzhen Mingtai Intelligent Technology Co., Ltd., Beijing Yin LIANJINKA TECHNOLOGY LIMITED.

The main drafters of this document are: Li Na, Wang Zhifei, Xu Yuwei, Zhao Yaru, Hao Mingqi, Mo Linmin, Peng Hong, Song Jingyan, Chang Jun, Li Chenxing, Wei Lili, Hou Han, Ma Danlei, Cheng Yong, Zhao Gang, Zhang Bo, Wang Xia, Yu Xin, Wu Shuyuan, Yang Shuang, Li Na, Liao Lelin, Hua Zirong, Zhang Xinliang, Wang Wenfeng, Dong Jingjing, Wang Xiaoyu, Zhang Wenjie, Gao Yan, Gai Shutian, Liu Bo, Long Mengmeng, Song Guodong, Lu Jun, Jiang Dong, Duan Kaizhi, Zheng Ying, Zhang Xuefei, Yu Hong.

Introduction

This document regulates the application practice of the social security card, focuses on the business needs of the social security card, and targets the physical social security Standardize the technology, quality control, application and management requirements of social security cards, electronic social security cards and one-card applications It is a basic

standard for realizing the social security card "one card for multiple uses, universal nationwide", supporting the government public service card, and the resident service card.

It plays an important basic guiding role.

GB/T 45498 "Specifications for the Social Security Card of the People's Republic of China" is the basis for regulating the work of the Social Security Card of the whole country.

The standard for the safety and universality of the project is planned to consist of four parts.

- Part 1: Basic specifications. The purpose is to specify the basic requirements for the social security card, including the Contents include system architecture, carrier requirements, service channels and basic support requirements.

- Part 2: Application Specification. The purpose is to specify the application requirements of the social security card, including the Platform basic requirements, application scenarios, application processes, platform access technology requirements, platform access management requirements, application collaboration and promotion Requirements, etc.

- Part 3: Security specifications. The purpose is to specify the security requirements of the social security card, including the Contents include carrier security requirements, terminal security requirements, platform security requirements, data security requirements and key security requirements.

- Part 4: Terminal Specification. The purpose is to specify the terminal requirements for the social security card, including the terminal requirements for the social security card Terminal form, basic terminal requirements, terminal technical requirements, etc.

Social Security Card of the People's Republic of China Part 3: Safety regulations

1 Scope

This document specifies the security system architecture, carrier security requirements, terminal security requirements, platform security requirements, data security requirements, etc. of the social security card.

According to security requirements and key security requirements.

This document applies to the design, development, integration, application, maintenance and operation of the social security card security system.

2 Normative references

GB/T 16649.4

GB/T 22239-2019

GB/T 25069-2022