ICS 35.240.40
CCS A11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21079.2-2022

Financial services - Secure cryptographic devices (retail) - Part 2: Security compliance checklists for devices used in financial transactions

金融服务 安全加密设备（零售）第2部分：金融交易中设备安全符合性检测清单

Issued on: December 30, 2022 **Implemented on: December 30, 2022**

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

Table of Contents

Foreword

This document was issued on 30 December 2022 by the State Administration for Market Regulation; Standardization Administration of the PRC and takes effect on 30 December 2022.

It is a GB/T standard: recommended rather than compulsory, but it is the text a Chinese reviewer applies when assessing a submission.

It is classified under ICS 35.240.40, Chinese classification A11.

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 2 of GB/T 21079 "Security Encryption Equipment for Financial Services (Retail)". GB/T 21079 has been issued

The following sections.

--- Part 1.Concepts, requirements and assessment methods.

This document replaces GB/T 20547.2-2006 "Banking Security Encryption Equipment (Retail) Part 2.Equipment in Financial Transactions

Safety Compliance Inspection List", compared with GB/T 20547.2-2006, except for structural adjustment and editorial changes, the main technical changes

as follows.

a) Added the term "evaluation body" (see 3.4);

b) Added "authorized quasi-formal assessment" (see 4.4);

c) The relevant requirements of my country's cryptographic algorithms have been added (see A21 of Table A.5, B18 of Table B.3 and E4 of Table E.2);

d) Some appendices have been added (see A.3.4, A.3.6, B.2.1.2).

This document is modified to adopt ISO 13491-2.2017 "Security Encryption Equipment for Financial Services (Retail) Part 2.Equipment in Financial Transactions

Safety Compliance Checklist".

Compared with ISO 13491-2.2017, this document has made the following structural adjustments.

---In Appendix H, the serial numbers H1~H5 of Table H.1 correspond to H4~H8 of Table H.1 in ISO 13491-2.2017;

---In Appendix H, the serial numbers H6~H8 of Table H.2 correspond to H1~H3 of Table H.2 in ISO 13491-2.2017.

The technical differences between this document and ISO 13491-2.2017 and their reasons are as follows.

---In appendix A, the serial number A21 of Table A.5, the description about the encryption algorithm, operation mode and key length is changed to "equipment use

The encryption algorithm, operation mode and key length shall comply with ISO 11568-1, ISO 11568-2, ISO 11568-4,

GB/T 32918, GB/T 32905 and GB/T 32907", in order to meet the relevant requirements of my country's password management department;

---In Appendix B, the serial number B18 of Table B.3, the description about the PINBlock format is changed to "PIN encryption shall adopt ISO 9564-

1, the PINBlock format specified in ISO 9564-1 shall adopt the encryption algorithm specified in ISO 9564-1 and the SM4 block cipher algorithm "to comply with

Relevant requirements of my country's password management department;

---In appendix E, the serial number E4 of Table E.2, the description of the key generation method is changed to "The key generation method shall comply with

ISO 11568 (all parts), GB/T 32918, GB/T 32905 and GB/T 32907", in order to comply with the password management department of our country

door related requirements.

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

This document is proposed and managed by the National Financial Standardization Technical Committee (SAC/TC180).

This document was drafted by. Beijing UnionPay Gold Card Technology Co., Ltd., China UnionPay Co., Ltd., Changsha Center of the People's Bank of China

branch.

The main drafters of this document. Yang Bo, Zhang Yanchao, Tan Yifu, Tong Dong, Tang Yang, Yuan Sisi, Tan Wang, Du Rui.

This document was first published in 2006, and this is the first revision.

Introduction

The security of retail electronic payment systems relies heavily on the security of secure encryption devices. Security Encrypted Device Security

The requirements are based on assumptions that computer files may be accessed and processed illegally, that communication lines may be "tapped" and that legitimate data and control

Control instructions may be replaced by illegal operations. Although some security encryption devices (such as host security modules) are placed in relatively high security places

However, most of the security encryption devices (such as PIN pads, etc.) used in retail banking are in an insecure environment. because

Therefore, when dealing with PIN (Personal Identification Number), MAC (Message Authentication Code), encryption keys and other confidential data on these secure encrypted devices, there are

Risk of device compromise, data leakage, or tampering.

The proper use and proper management of secure cryptographic devices with specific physical and logical security features can help reduce financial risk.

Internationally, the ISO 13491 series of standards are the reference and basis for the use, management and evaluation of various security encryption devices in the financial transaction process.

universal basic standard. According to the security requirements for secure encryption devices (hereinafter referred to as SCD) in ISO 13491-1, ISO 13491-2.

2017 is based on ISO 9564-1, ISO 9564-2, ISO 16609, ISO 11568-1, ISO 11568-2 and ISO 11568-4 and other standards.

A security compliance checklist for assessing SCDs in a financial services environment. Our country learns from the ISO 13491 series standards and combines our country's password

Relevant requirements of management departments and financial industry authorities form GB/T 21079 "Security Encryption Equipment for Financial Services (Retail)", guiding gold

The evaluation of security encryption equipment in the retail business of the financial industry is planned to be composed of two parts.

--- Part 1.Concepts, requirements and assessment methods. It is designed to provide for the protection of messages, keys and other sensitive data in financial retail business

The physical characteristics, logical characteristics and management requirements of the SCD of the data include the security requirements for the SCD.

--- Part 2.Checklist for equipment security compliance in financial transactions. Designed to provide security symbols for evaluating secure cryptographic devices

Compliance testing list, including the characteristics that the equipment must have, the characteristics of the equipment operating environment and the management methods of the equipment. exist

Other assessment frameworks are also suitable for formal safety assessments, for example. ISO /IEC 15408 Parts 1 to 3 and

ISO /IEC 19790, but these are beyond the scope of this part of GB/T 21079.

China's retail financial business is in a period of rapid development, and security encryption equipment is very important to ensure the security of retail financial business.

This document provides a security compliance checklist for evaluating security encryption equipment, which helps to improve the security of security encryption equipment in the financial industry

Management level, and provide guidance for the standardization and normalization of security assessment work related to security encryption equipment.

Financial Services Security Encryption Device (Retail)

Part 2.Equipment security in financial transactions

Compliance Checklist

1 Scope

GB/T 21079.2-2022 turns the security requirements for retail payment cryptographic