ICS 35.240.40
CCS A 11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21079.1-2022

Replacing GB/T 21079.1-2011

Financial services - Secure cryptographic devices(retail) - Part 1: Concepts, requirements and evaluation methods

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

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Preface
Introduction
1 Scope 1
2 Normative references 1
3 Terms and Definitions 1

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

The following sections.

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

This document replaces GB/T 21079.1-2011 "Banking Security Encryption Equipment (Retail) Part 1.Concept, Requirements and Evaluation

Compared with GB/T 21079.1-2011, except for structural adjustment and editorial changes, the main technical changes are as follows.

a) Delete terms such as "certification report" and "initiating agency" (see Chapter 3 of GB/T 21079.1-2011);

b) Added "accredited certification body" (see 3.3), "approval agency" (see 3.4), "approval letter" (see 3.5), "assessment certificate" (see

3.11), "device management" (see 3.16), "dual control" (see 3.17), "financial key" (see 3.22), "hardware security module" (see

3.24), "key loading device" (see 3.25), "security scheme" (see 3.30), "sensitive function" (see 3.32) and other terms;

c) Added "anti-attack requirements" (see 6.3), "anti-attack requirements" (see 6.4), "anti-attack requirements" (see 6.5);

d) Change the logical safety requirements of SCD (see 6.6);

e) Added "SCD shall support the use of SM2 elliptic curve public key cryptographic algorithm, SM3 cryptographic hash algorithm and SM4 block cipher

Algorithm, complying with the requirements of GB/T 32918, GB/T 32905 and GB/T 32907" (see 6.6.5);

f) Changed the equipment life cycle stage and corresponding protection requirements (see 7.2, 7.3);

g) Deleted the informative appendix A "Concepts related to system security level" (see Appendix A of GB/T 21079.1-2011), deleted

Text "8 Assessment methods" (see Chapter 8 of GB/T 21079.1-2011);

h) Added informative Appendix A "Assessment Method" (see Appendix A).

This document is modified to adopt ISO 13491-1.2016 "Security Encryption Equipment for Financial Services (Retail) Part 1.Concepts, requirements and evaluation

Estimation Method".

Compared with ISO 13491-1.2016, this document has made the following structural adjustments.

--- 3.4~3.37 in Chapter 3 correspond to 3.3~3.36 of ISO 13491-1.2016.

The technical differences between this document and ISO 13491-1.2016 and their reasons are as follows.

---Chapter 3 adds "accredited certification body" (see 3.3), which complies with the relevant requirements of the Regulations of the People's Republic of China on Certification and Accreditation;

---In Chapter 6, 6.6.5 adds "SCD shall support the use of SM2 elliptic curve public key cryptographic algorithm, SM3 cryptographic hash algorithm and

SM4 block cipher algorithm, in line with the requirements of GB/T 32918, GB/T 32905 and GB/T 32907" description, in line with I

Relevant requirements of the national encryption management department;

--- A.1.5 in Appendix A modifies the formal evaluation process (see Figure A.1), which complies with the relevant regulations of the "Regulations of the People's Republic of China on Certification and Accreditation"

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.

Introduction

The security of retail electronic payment systems relies heavily on the security of secure encryption devices. Security is proposed based on this

Some assumptions are made. computer files may be accessed and processed illegally, communication lines may be "wiretapped", and legitimate data and control instructions may be

replaced by illegal operations. Handle PINs (Personal Identification Numbers), MACs (Message Authentication Codes), keys, and other secrets on these encrypted devices

There is a risk of data leakage or tampering. Security with specific physical and logical security features through reasonable use, proper management

Encrypted devices help reduce financial risk.

In order to ensure the orderly development of evaluation activities of secure encryption devices (SCDs), promote the rational use and management of SCDs, and establish corresponding security

Fully encrypted device evaluation criteria became a top priority. Internationally, the ISO 13491 series of standards belong to various security measures in the process of financial transactions.

The use, management and evaluation of encrypted equipment are referenced and based on general basic standards, of which ISO 13491-1.2016 is based on ISO 9564,

ISO 16609, ISO 11568 and other standards stipulate the security encryption used to protect messages, keys and other sensitive information in financial retail services

The characteristics and management requirements of the device. Our country draws on the ISO 13491 series of standards, and combines our country's password management department and financial industry department

Relevant requirements of the door, form GB/T 21079 "Financial Service Security Encryption Equipment (Retail)", guide the security encryption in the retail business of the financial industry

Equipment evaluation is proposed 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, including 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 regulates the physical characteristics, logical characteristics and management requirements of SCD applied in the financial retail business, in order to improve

High SCD's own security and management level are very useful in maintaining financial market order, strengthening financial stability in the market, and protecting the security of financial activities.

Is of great significance.

Financial Services Security Encryption Device (Retail)

Part 1.Concepts, requirements and assessment methods

1 Scope

This document specifies the concept of secure encryption devices, as well as the requirements for device security features and device management.

This document applies to the security management of SCD equipment used in retail financial services.

This document does not apply to problems caused by SCD denial of service.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, dated references

For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to

this document.

GB/T 32905 Information Security Technology SM3 Cryptographic Hash Algorithm

GB/T 32907 Information Security Technology SM4 Block Cipher Algorithm