ICS 35.240.40
CCS A 11

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 21078.4-2023

Financial services - Personal Identification Number (PIN) management and security - Part 4: Approved algorithms for PIN encipherment

Issued on: March 17, 2023 **Implemented on: March 17, 2023**

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

Table of Contents

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 4 of GB/T 21078.GB/T 21078 has issued the following parts.

---Financial Services Personal Identification Number Management and Security Part 1.PIN Basic Principles and Requirements Based on Card System

(GB/T 21078.1);

--- Banking Personal Identification Number Management and Security Part 3.Guidelines for PIN Processing in Open Networks (GB/T 21078.3);

--- Financial Services Personal Identification Number Management and Security Part 4.Approved PIN Encryption Algorithms (GB/T 21078.4).

This document is modified to adopt ISO 9564-2.2014 "Financial Services Personal Identification Number Management and Security Part 2.Approved PIN plus

Encryption Algorithm".

Compared with ISO 9564-2.2014, this document has made the following structural adjustments.

--- Increased "Terms and Definitions" chapter (see Chapter 3).

The technical differences between this document and ISO 9564-2.2014 and the reasons are as follows.

--- Changed the normative reference documents, and replaced ISO 9564-1 with GB/T 21078.1-2023 (see Chapter 2) to adapt to my country's

Technical conditions;

--- The SM4 block cipher algorithm (see Chapter 7) has been added to adapt to domestic practical applications.

The following editorial changes have been made to this document.

--- Added notes on the definition and use of the algorithm to facilitate reading.

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 under the jurisdiction of the National Financial Standardization Technical Committee (SAC/TC180).

Introduction

GB/T 21078 aims to specify the basic principles and requirements of PIN management and security in financial services, and is intended to be composed of three parts.

--- "Financial Services Personal Identification Number Management and Security Part 1.Basic Principles and Requirements of PIN Based on Card System"

(GB/T 21078.1), which aims to provide the basic principles and techniques for the minimum security measures required for effective PIN management.

--- "Management and Security of Personal Identification Numbers in Banking Services Part 3.Guidelines for PIN Processing in Open Networks" (GB/T 21078.3), aimed at

Define minimum PIN security guidelines in an open network environment.

--- "Financial Services Personal Identification Number Management and Security Part 4.Approved PIN Encryption Algorithms" (GB/T 21078.4), aimed at

Define approved PIN encryption algorithms and requirements for their use.

It has been more than ten years since the first part of GB/T 21078 was released in.2007.During this period, the application of PIN in financial services has continued to deepen.

Changes have also taken place in the management and security requirements for PIN and related international standards.

---ISO 9564-1.2002 adopted by GB/T 21078.1-2007 was revised twice in.2011 and.2017.

GB/T 21078.1-2007 was replaced by GB/T 21078.1-2023;

---GB/T 21078.2-2011 revised ISO 9564-3.2003 which was merged into ISO 9564-1 in.2011,

ISO 9564-3.2003 has been abolished, and GB/T 21078.2-2011 is replaced by GB/T 21078.1-2023;

---GB/T 21078.3-2011 equivalently adopts ISO /T R9564-4.2004 to provide security for PIN in an open network environment

Protect;

--- This document is modified to adopt ISO 9564-2.2014 to supplement the blank of the approved PIN encryption algorithm and adapt to the continuously generated passwords

Algorithm application new requirements.

This document, on the basis of meeting the application requirements of international cryptographic algorithms, combined with the actual application of cryptographic algorithms in my country, includes the following

Approval Algorithm for Password PIN.

--- Triple data encryption algorithm;

---RSA encryption algorithm;

---AES encryption algorithm;

--- SM4 block cipher algorithm.

Financial Services PIN Management and Security

Part 4.Approved PIN Encryption Algorithms

1 Scope

This document applies to the scenario where the PIN is encrypted and protected.

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 21078.1-2023 Financial Services Personal Identification Number Management and Security Part 1.PIN Basic Principles Based on Card System

Rules and requirements (ISO 9564-1.2017, MOD)

GB/T 32907 Information Security Technology SM4 Block Cipher Algorithm

ISO /IEC 18033-2 Information Technology Security Technology Encryption Algorithms Part 2.Asymmetric Cryptography (Information

ISO /IEC 18033-3 Information Technology Security Technology Encryption Algorithms Part 3.Block Ciphers (Information

3 Terms and Definitions

This document does not have terms and definitions that need to be defined.

4.1 Definition

Describe the definition.

Note. TDEA is a kind of symmetric algorithm.

4.2 use

When using the TDEA defined by ISO /IEC 18033-3, the TDEA key option is 1 or 2 to GB/T 21078.1-2023

When encrypting the PIN data block described in, TDEA shall run on the Electronic Codebook (Electronic Codebook) specified in ISO /IEC 10116.

CodeBook, ECB) mode (where the packet size n is 64).

This encryption algorithm is only approved for formats 0, 1 and 3 of the PIN data block.

Note. Please refer to 10.3.2 of GB/T 21078.1-2023 for the relevant content of PIN data block format 0, and see GB/T 21078.1-2023 for relevant content of format 1