

ICS 35.240.40

CCS A 11



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

GB/T 21078.1-2023

Replacing GB/T 21078.1-2007, GB/T 21078.2-2011

**Financial services - Personal Identification Number(PIN)
management and security - Part 1: Basic principles and
requirements for PINs in card-based systems**

Issued on: March 17, 2023

Implemented on: March 17, 2023

**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	2

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 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 replaces GB/T 21078:1-2007 "Management and Security of Personal Identification Numbers in Banking Services - Part 1: ATM and

Basic Principles and Requirements for Online PIN Processing in POS System" and GB/T 21078:2-2011 "Management of Banking Personal Identification Codes

and Security Part 2: Requirements for Offline PIN Processing in ATM and POS Systems: This document is based on GB/T 21078:1-2007

Mainly, it integrates the content of GB/T 21078:2-2011: Compared with GB/T 21078:1-2007, except structural adjustment and editorial changes

In addition, the main technical changes are as follows:

- a) Changed the name of the standard (see the cover, the cover of the:2007 edition);
- b) Added terms "cardholder PIN", "integrated circuit", "integrated circuit card", "primary

account payment token", "sensitive status" (see Section 3 chapter);

c) The terms "irreversible encryption", "irreversible transformation of a key", "key component", "notarization", "key splitting", "key variant" are removed (see Chapter 3 of the:2007 edition);

d) Added the chapter "Abbreviations" (see Chapter 4);

e) Added an overview of the basic principles of PIN management, introducing and comparing the concepts of "cardholder PIN", "reference PIN" and "transaction PIN" (see 5:1);

f) Changed part of the basic principles of PIN management (see 5:2, Chapter 4 of the:2007 edition);

g) Added security requirements for PIN processing equipment (see 6:1) and physical security matters for IC card readers (see 6:2);

h) Deleted the input requirements of PIN (see 5:3 of the:2007 edition), and the matters to be considered during packaging (see 5:4 of the:2007 edition);

i) Changed the title of the article to "PIN processing system" and adjusted the relevant requirements (see 7:1:1, 6:1:1 of the:2007 edition);

j) Changed the recording media requirements (see 7:1:2, 6:1:2 of the:2007 edition), oral communication requirements (see 7:1:3, :2007 edition

6:1:3);

k) Changed part of the content of PIN encryption, including adding the requirement of offline PIN (see 7:2, 6:2 of the:2007 edition);

l) The physical security requirement of PIN is deleted (see 6:3 of the:2007 edition);

m) Increased PIN verification requirements (see Chapter 8);

n) Changed the title of the article titled "PIN establishment" (see 9:2, 7:2 of the:2007 edition); added the requirements for "PIN selection" (see 9:4), "PIN

Replacement" requirements (see 9:6), "PIN letter" requirements (see 9:11);

o) Added the PIN protection requirements when sending to the IC card for offline PIN verification, and merged GB/T 21078:2-2011

Partial content (see 10:2:2);

p) Changed section title to "Compressed PIN block format" (see 10:3, 8:3 of version:2007); added "PIN number for format 2

"Data block" is used in offline environment, which merges part of the content of GB/T 21078:2-2011 (see 10:3:4); adds "compressed PIN

"Restrictions on the use of the data block format" (see 10:3:6);

q) Added the relevant requirements of "extended PIN data block" (see 10:4);

r) Added the relevant requirements of "Conversion Restriction of PIN Data Block Format" (see 10:5);

s) Added relevant requirements for "transaction log containing PIN data" (see 10:6);

t) Part of the content of "Destruction of Sensitive Data" has been changed (see Appendix A, Appendix F of the:2007 edition);

u) Changed part of the "PED Design Guidelines" (see Appendix B, Appendix E of the:2007 edition);

v) Part of the content of "Information Provided to Customers" has been changed (see Appendix C, Appendix G of the:2007 edition);

w) Deleted "General Principles of Key Management" (see Appendix A of the:2007 Edition), "PIN Verification Technology" (see Appendix A of the:2007 Edition

B), "PIN input device for online PIN encryption" (see Appendix C of the:2007 edition), "Pseudo-random PIN generation example"

(See the relevant content of Appendix D of the:2007 edition):

This document is modified to adopt ISO 9564-1:2017 "Financial Services Personal Identification Number Management and Security Part 1: Card-based system

PIN Basic Principles and Requirements":

Compared with ISO 9564-1:2017, this document has made the following structural adjustments:

--- Increased "Abbreviations" chapter (see Chapter 4):

The technical differences between this document and ISO 9564-1:2017 and their reasons are as follows:

---Changed the normative reference documents and replaced ISO 9564-2 with GB/T 21078:4-2023 to adapt to the technical conditions of our country;

--- The PIN data block of format 4 is added to support the SM4 block cipher algorithm (see 10:4:1), so as to adapt to the actual domestic application:

The following editorial changes have been made to this document:

--- Deleted the terms "irreversible encryption", "key components" and "key splitting",

because in this document except for the chapter "Terms and Definitions" and

Not mentioned;

--- Added the abbreviations of "host security module" and "secure cryptographic device" (see Chapter 4) for ease of use;

--- Deleted the informative references NIST/SP800-22 and NIST/SP800-88 to adapt to the actual domestic application:

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 21078:2-2011 revised ISO 9564-3:2003 which was merged into ISO 9564-1 in:2011,

ISO 9564-3:2003 has been abolished;

---GB/T 21078:3-2011 equivalently adopts ISO /T R9564-4:2004 to provide security for PIN