

ICS 35.240.40
CCS A 11



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

GB/T 21078.2-2011

**Banking -- Personal identification number management and
security -- Part 2: Requirements for offline PIN handling in ATM
and POS systems**

银行业务 个人识别码的管理与安全 第2部分：ATM和POS系统中脱机PIN处理的要求

(English Translation)

Issued on: December 30, 2011

Implemented on: February 1, 2012

Issued by: Standardization Administration of China

Table of Contents

Introduction

Introduction

1 Scope

2 Normative references

3 Terms and definitions

Between PIN 4 PIN Entry Device (PED) and the IC card reader transmission protection

5 Physical Security

6 PINBLOCK format

6.1 Overview

PINBLOCK 6.2 format 2

Reference

Foreword

GB/T 21078 "Banking - Personal Identification Number management and security" is divided into the following three parts.

--- The first part 1. ATM and POS systems basic principles and requirements for online PIN processing;

Part --- Article 2. ATM and POS systems offline PIN processing requirements;

--- Part 3. Guidelines for PIN handling in open networks.

This section GB/T 21078 Part 2.

This section drafted in accordance with GB/T 1.1-2009 given rules.

The partial modification of the use of ISO 9564-3:2003 "Banking - Personal Identification Number management and security - Part 3. ATM and POS system offline PIN processing requirements "(in English).

This part of ISO 9564-3:2003 is a technical difference. According to the practical application of the domestic situation, the 6.1 "should each transaction Use only key "requirements expanded to" use unique key per transaction or periodic replacement of the encryption key. "For technical differences it has been incorporated in the text and it relates to the terms of the margin of a single vertical line identification.

This part of ISO foreword deleted.

This section proposed by the People's Bank of China.

This part of the National Standardization Technical Committee on Finance (SAC/TC180) centralized.

This section is responsible for drafting units. China Financial Computerization Corporation.

Participated in the drafting of this section. Industrial and Commercial Bank of China, Bank of China, Bank of Communications, China People's Bank branch in downtown Xinghua, China silver Union Company.

Introduction

Built-in IC card financial transactions in the technology can be used IC card PIN verification offline. Currently issuer can choose Offline or online manner PIN verification. GB/T 21078 is offline PIN This section sets out clear requirements.

Offline PIN verification does not require the cardholder's PIN is sent to the card issuer host authentication, so be PIN protected by a network phase Off safety requirements do not apply. However, despite the offline PIN verification, many common PIN protection principles and techniques still apply.

GB/T 21078 in this section gives specific requirements for offline PIN handling class, unless explicitly stated, GB/T 21078.1-2007 to the basic principle of the PIN management apply to this section.

ISO Part 610 202 defines the use of IC card for cardholder verification of safety requirements. It should be noted that, ISO 10202 definitions the requirements of the IC card itself, rather than on the IC card acquirer to accept the requirements of the equipment, it can be seen as a complement to the GB/T 21078 of.

Banking - Personal Identification Number management and security Part 2. ATM and POS systems offline PIN Processing requirements

1 Scope

This section specifies the minimum safety requirements for offline PIN processing and standard method for exchanging PIN data in an offline environment.

This section applies to require an offline PIN verification initiated financial transaction card, also applies to those responsible for the ATM acquirer and laying Institutions PIN management and protection technologies implemented in the POS terminal.

This section does not apply to the following situations.

a) PIN management and security online PIN environment, GB/T 21078.1 contains the contents;

- b) Approved PIN encryption algorithm;
- c) the use of PIN in an open network environment, GB/T 21078.3 contains the contents;
- d) to prevent the user or card issuer and its agents authorized employee misuse lost or intentionally taken with PIN protection;
- e) the privacy of non-PIN transactions;
- f) protection of transaction messages against modification or replacement, such as online authorization response;
- g) to prevent the PIN or transaction replay;
- h) a specific key management;
- i) IC card is encrypted PIN accepted decisions;
- j) non-contact IC card.

GB/T 21078.1-2007 Chapter 4 of the basic principles of PIN management described also apply to this section.

And multi-application IC card-related requirements by the card issuer is responsible, is not included in this section.

This section applies to IC card technology, but not limited to IC card technology.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB/T 16649 (all parts) Identification cards contact IC card (ISO/IEC 7816-1:1998, MOD)
GB/T 21078.1-2007 Banking Personal Identification Number management and security - Part 1. ATM and POS systems in the United the basic principles and requirements for machine PIN processing (ISO 9564-1:2002, MOD) EMV2000 payment system integrated circuit card specifications - Volume 2. Security and Key Management (version 4.0) 2000.12 (EMV2000, IntegratedCircuitCardSpecificationforPaymentSystems, Book2-SecurityandKeyManagement, Version 4.0, December, 2000)

3 Terms and Definitions

GB/T 21078.1-2007 and as defined in the following terms and definitions apply to this document.

Integrated circuit (IC) integratedcircuit (IC) According to GB/T 16649 in the provisions of (typically) a microprocessor embedded in the IC card.