

ICS 35.030
CCS L 80

GM

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

GM/T 0106-2021

Cryptograph application requirements for bank card terminal

银行卡终端产品密码应用技术要求

(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
General	4
General requirements	5
Requirements for POS terminals	6
Requirements for ATM terminals	7
Requirements for cryptographic modules	8
Key system	9
Terminal master key management	10
Key encryption key management	11
Working key management	12
Certificate authority public key management	13
Certificate authority public key maintenance key management	14
Terminal security key management	15
Self-checking	16
Sensitive function use authorization	17
Online transaction messages	18
Offline data authentication	19
Cash dispense cryptographic authentication	20
Cryptographic algorithm correctness and performance	21

1 Scope

This document specifies the technical requirements for the cryptographic application on bank card terminal products, including basic terminal security requirements, terminal key management requirements, terminal data security requirements, and cryptographic algorithm correctness and performance requirements.

This document applies to the application of cryptographic technology on bank card terminal products. The users are mainly the units that design, manufacture, and use bank card terminal products related to the application of cryptographic technology, as well as the relevant units that need to upgrade the cryptographic application technology of existing bank card terminal products.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 21078.1, Financial services - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for PINs in card-based systems GB/T 21078.2, Banking - Personal identification number management and security - Part 2: Requirements for offline PIN handling in ATM and POS systems GB/T 27909 (all parts), Banking - Key management (retail) GB/T 32905, Information security techniques - SM3 cryptographic hash algorithm GB/T 32907, Information security technology - SM4 block cipher algorithm GB/T 32915, Information security technology - Binary sequence randomness detection method GB/T 32918 (all parts), Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 32918.3-2016, Information security techniques - Elliptic Curve public-key cryptography - Part 3: Key exchange protocol GM/T 0008, Cryptography test criteria for security IC GM/T 0028-2014, Security requirements for cryptographic modules GM/Z 4001, Cryptology terminology JR/T 0025.6, China financial integrated circuit card specifications - Part 6:

Debit/credit application terminal specification JR/T 0025.7, China financial integrated circuit card specifications - Part 8: Contact less specification independent of application JR/T 0055 (all parts), Technical specifications on bankcard interoperability JR/T 0120.1, Security specification for bank card terminals - Part 1: Port of sale terminal JR/T 0120.3, Security specification for bank card terminals - Part 3: Self-service terminal JR/T 0120.5, Security specification for bank card terminals - Part 5: PIN entry device ANSI X9.24 (all parts), Retail financial services - Symmetric key management

3 Terms and definitions

For the purposes of this document, the following terms and definitions, as well as those given in GM/Z 4001 and GM/T 0028, apply.

cash handling module the cash dispense module or cash recycle module of an Automatic Teller Machine (ATM).

bank card terminal

terminal

Commercial device - such as ATM, POS, mPOS and other products - that accepts bank card transactions.

secure communication key Symmetric key used to encrypt communication between

cryptographic modules within the terminal.

3.11

root public key

The public key of a certificate authority (CA), which is often used to verify the public key certificates or public key signatures issued by the certificate authority to itself, subordinate certificate authorities, or other clients.

3.12

root certificate

The unsigned or self-signed public key certificate issued by the certificate authority (CA) to itself, which is the starting point of the trust chain.

3.13

PIN entry device; PED A cryptographic module - such as encrypting pin pad (EPP), external encrypted pin pad, etc. - that supports personal identification number input.

3.14

encrypting pin pad; EPP A cryptographic module that accepts the user PIN entry and provides the cryptographic services required by the terminal.

3.15

external encrypted pin pad A PIN entry device that is used in the financial payment field, which can be a POS or an encrypting pin pad commonly used to connect to a POS to accept bank card transactions.

3.16

safety box

A device, inside the ATM, in which the cash handling module is placed, which is used to physically protect the cash handling module and cash.

cryptographic modules in terms of hardware, physical security, logical security and business functions, and is the basis for implementing the application of cryptographic technology.

5.2.1 General

Bank card terminal products are terminal devices for accepting bank card business, including point of sale (POS) products (POS, mPOS, smart POS, etc.) and automatic teller machine (ATM) products (ATM, financial self-service equipment, etc.). Bank card terminals shall include cryptographic modules, such as including encrypting pin pad, external

encrypted pin pad, etc., or being cryptographic modules themselves.

5.2.2 General requirements

The provisions in JR/T 0025.6-2018 and JR/T 0025.7-2018 shall be met.

The provisions in GM/T 0028-2014 shall be met and the cryptographic boundaries shall be divided.

The cryptographic algorithms given in GB/T 32905, GB/T 32907, and GB/T 32918 (all parts) shall be supported and executed by the cryptographic module of the terminal.

5.2.3 Requirements for POS terminals

The requirements of JR/T 0120.1 shall be met.

5.2.4 Requirements for ATM terminals

The requirements of JR/T 0120.3 shall be met.

5.3 Requirements for cryptographic modules

The cryptographic module on the bank card terminal product shall comply with the security requirements specified in GM/T 0028 and reach security level 1 or higher. It shall be provided with the function of generating random numbers and support the cryptographic algorithms specified in GB/T 32905, GB/T 32907 and GB/T 32918.

These cryptographic algorithms shall be provided by the security chip. The cryptographic module shall use the security chip approved by the national cryptographic management department, and the security level of the security chip shall reach the security level 2 specified in GM/T 0008.

Bank card terminals may contain multiple cryptographic modules. If data exchange is required between cryptographic modules, the confidentiality and integrity of sensitive data shall be guaranteed, such as using secure communication key encryption and communication with a message authentication code (MAC).

All keys of the terminal shall be stored in the cryptographic module, and the keys shall only be used in the cryptographic module.

6.3.1 Key system

The key system used by bank card terminals for online transactions shall be no less than two levels.

POS terminals often use a two-level key system: terminal master key (TMK) and working key (WK).