

ICS 35.030
CCS L 80

GM

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

GM/T 0107-2021

**Smart IC card key management system basic technical
requirements**

智能IC卡密钥管理系统基本技术要求
(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
Overview	3
Overview	4
System management function	5
Symmetric key management function	6
Asymmetric key management function	7
Interface service function	8
Overview	9
Key generation	10
Key diversify	11
Overview	12
Key generation	13
Key distribution	14
Key storage	15
Key backup	16
Cryptographic algorithms	17
Cryptographic module	18

1 Scope

This document specifies the application architecture and key system, functional requirements, key security mechanism, system security requirements, etc. of the smart IC card key management system.

This document is applicable to the design, development, testing, use of the smart IC card key management system.

2 Normative references

The contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, 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 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32907 Information security technology - SM4 block cipher algorithm GB/T 32915 Information security technology - Randomness test methods for binary sequence GB/T 32918 Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 36322 Information security technology - Cryptographic device application interface specifications GB/T 39786 Information security technology - Baseline for information system cryptography application GM/T 0044 SM9 identification cryptographic algorithm GM/T 0045 Specifications of financial cryptographic server GM/T 0051 Cryptography device management - Specifications of symmetric key management technology - Smart IC card key management system on the issuer side: responsible for importing certificates and keys from superior institutions, generating and managing smart IC card business keys and institution certificates of this level, providing key services for smart IC card issuance and transactions;

- Smart IC card acceptance terminal: a terminal that processes smart IC card transactions (including POS, ATM, gate, on-board terminal, etc.). The acceptance terminal imports the smart IC card business root public key certificate or the PSAM card containing the smart IC card consumer key root key; completes offline authentication with the smart IC card through these certificates or public keys;

- Smart IC card management system: a system that manages smart IC card business data; provides services for smart IC card issuance and transactions. The smart IC card management system deploys smart IC card transaction keys (electronic wallet keys or electronic cash keys); completes online authentication with smart IC cards through these keys;

- Smart IC card clearing and settlement system: a system that handles the clearing and settlement of smart IC card transactions. The smart IC card clearing and settlement system deploys smart IC card settlement keys; completes transaction authentication during smart IC card clearing and settlement through these keys;

- Data preparation system: process the business data and security data required for smart IC card issuance; form the final card making file. The data preparation system contains information such as smart IC card certificates and smart IC card keys;

- SAM card issuance system: execute the SAM card issuance process; safely load relevant keys and files into the SAM card after security authentication. The smart IC card consumption root key and SAM card management key are deployed in the SAM card issuance system;

- User card issuance system: execute the user card issuance process; securely load relevant keys and files into the user card after security authentication; deploy the user card business key in the user card issuance system.

5.2.1 Overview

The keys involved in the smart IC card key management system can be divided into smart IC card business keys and system protection keys, according to the key purpose or key source.

Smart IC card business keys are defined by the smart IC card application specification.

6.1 Overview

The smart IC card key management system mainly generates and manages the root key and corresponding certificates of smart IC card services; provides key service functions for other smart IC card related systems, which shall at least include system management, symmetric key management, asymmetric key management, audit management, interface service and other functions.

6.2 System management function

The system management function shall be responsible for user role authority management, operator management, system configuration management, device management functions.

- a) Role authority management: It shall include authority resource management and user management; it shall be used to add, delete, modify, check, set permissions and other operations to assign appropriate permissions to the corresponding roles.
- b) Operator management: Users with different permissions shall be divided according to roles; different roles shall be assigned to operators. It is used to add, delete, modify, check system operators; assign corresponding roles to operators when creating operators.
- c) System configuration management: It shall implement various system configurations for managing the smart IC card key management system, including various basic information and business information configurations.
- d) Equipment management: It shall implement encryption machine management of the smart IC card key management system, including the maintenance of encryption machine resource information, reasonable grouping management of encryption machine resources, monitoring and management functions of encryption machines. It shall support the addition, modification, viewing, deletion and other operations of encryption machines to complete the configuration management of encryption machines.

6.3 Symmetric key management function

The symmetric key management function shall support the generation, storage, use, destruction of various symmetric key types, including the security management of keys stored in encryption machines and keys stored in databases; support the management of key attributes and key status of symmetric keys.

a) Generate/inject keys: The function of adding keys shall be implemented. The information of the added symmetric key should include but is not limited to the key name, expiration date, key type, key index, key version number, storage method, etc. If the key is added in ciphertext, the decryption key, decryption algorithm, key value and other related information shall be added.

b) Key diversify: During the use of keys, different levels of diversify will be performed. During the key addition process, the level of diversify to be used and the composition of the diversify factors at different levels shall also be defined.

The key diversify mechanism is shown in 7.1.3.

c) Update key: The added key information shall be queried and modified and saved.

d) Export key: The added key information shall be queried; the related information can be exported and backed up. The exported key can be protected by password envelopes or key transfer cards.

e) Key destruction: The information of symmetric keys shall be queried according to the conditions; symmetric keys that have expired, been leaked, or are no longer used for other reasons shall be deleted.

f) Expired key management: The key validity period shall be modified for keys that have expired or are about to expire.

6.4 Asymmetric key management function

The asymmetric key management function shall support the generation, storage, use, destruction of various asymmetric types of keys, including the security management of keys stored in encryption machines and keys stored in databases; it can support the management of key attributes and key status of asymmetric keys. At the same time, it shall support the management of related certificates and be responsible for the issuance and verification of certificates. It mainly includes but is not limited to the functions of generating certificate requests, importing/exporting certificates, destroying certificates.

a) Generate asymmetric key pairs: The function of generating key pairs can be supported. The parameters of asymmetric key pairs shall be different. When generating key pairs, different parameters shall be used to guide the generation of key pairs.

b) Import asymmetric key pairs: It shall support the import of generated key pairs into the smart IC card key management system for use.

c) Export asymmetric key pairs: It shall support exporting the generated key pairs to the smart IC card key management system, with the private key in encrypted of the event, the operation type, the operation result shall be recorded. The log shall be classified or comprehensively queried by time, operator, operation type, etc. Digital signatures and other methods shall be used to ensure that the log is not tampered with.