

ICS 35.030
CCS L 80

GM

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

GM/T 0124-2022

**Cryptography test specification for secure separation and
information exchange product**

安全隔离与信息交换产品密码检测规范

(English Translation)

Issued on: November 20, 2022

Implemented on: June 1, 2023

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Test requirements	4
Test method	5
Test requirements	6
Test method	7
Test requirements	8
Test method	9
Test requirements	10
Test requirements	11
Test method	12
Test requirements	13
Test method	14
Test requirements	15
Test method	16
Test requirements	17
Test method	18
Test requirements	19
Test method	20
Test requirements	21
Test method	22
General requirements	23
Test requirements	24
Test method	25
Test requirements	26
Test method	27
Product performance test	28
System framework	29

1 Scope

This document specifies the cryptography test contents, test requirements, test methods and documentation requirements for secure separation and information exchange products.

This document applies to the test of secure separation and information exchange products, as well as the development of such products.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 15843 (all parts) Information technology - Security techniques - Entity authentication
GB/T 20279-2015 Information security technology - Security technical requirements of network and terminal separation products
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 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves
GM/T 0062 Random number test requirements for cryptographic modules
GM/Z 4001-2013 Cryptology terminology

3 Terms and definitions

For the purpose of this document, the terms and definitions defined in GM/Z 4001 and the following apply.

Inspect the appearance, size, internal components and accessories of the product according to the physical parameters of the product.

4.3.1 Test requirements

The product shall use a management interface independent of the working interface for product management. The management interface should support the following main management functions:

- a) Product installation and initialization, system startup and shutdown, backup and recovery functions;
- b) Product dual-machine hot standby or load balancing and other availability parameter settings;
- c) If the product supports remote management, it shall have the ability to close the remote management interface, it shall restrict the addresses that can be remotely managed, and it

shall carry out remote management by establishing a secure channel. The cryptographic protocol used in the secure channel shall comply with relevant national cryptographic management regulations;

d) Product status query function management, including product configuration algorithm, key management, hardware cryptographic component status, etc.;

e) Log management functions, including log recording, log query, log export, etc.

4.3.2 Test method

Inspect the management functions supported by the product through the product management interface.

4.4.1 Test requirements

The product should have an initial status and a ready status, and can only be converted from the initial status to the ready status.

4.4.2 Test method

The test method is as follows.

a) After the product is powered on for the first time, it enters the initial status; at this time, the product cannot provide separation services for the two security domains.

After the product completes self-test and the administrator configures the network configuration, switching policy, security policy, etc., it enters the ready status.

b) After the product completes the initialization configuration, powers on and passes the product self-test, it enters the ready status and provides separation services.

4.5.1 Test requirements

The test requirements are as follows.

a) The product shall support the self-test function, which shall include the cryptographic algorithm correctness, random number quality, authentication data, key and information transmission policy (security attributes) integrity self-test, etc. Among them, the random number quality self-test shall meet the requirements of E products in GM/T 0062.

b) The product shall support power-on self-test, periodic self-test and conditional self-test functions.

4.5.2 Test method

The test method is as follows.

a) After the product is powered on, it automatically performs the power-on self-test.

If the self-test is successful, the product automatically enters the ready status; if the self-test fails, the product logs and issues an alarm.

b) During operation, the product automatically performs periodic self-tests according to the set cycle. If the self-test fails, the product logs and issues an alarm.

c) During operation, the product performs self-tests according to conditions. If the self-test fails, the product logs and issues an alarm.

4.6.1 Test requirements

The test requirements are as follows.

a) The product shall include but not be limited to management functions such as product permission configuration, network configuration, and access control configuration.

b) The permission configuration should:

1) support 2 serial ports (RJ45 or DB9 form) as management control ports;

2) support redundant power supply;

4.7.3.1 Test requirements

If the product uses the asymmetric cryptographic algorithm, it shall support the SM2 cryptographic algorithm, and its implementation shall comply with GB/T 32918 (all parts); the product shall be able to use the SM2 algorithm to perform operations such as encryption and decryption, signing/verification of data, and shall be able to support given keys and plaintext (ciphertext) to test the correctness of its operation results.

4.7.3.2 Test method

For the encryption and decryption operations that support the SM2 algorithm:

a) After the product uses the cryptographic algorithm to encrypt the given key and plaintext, the test platform performs a decryption operation on the ciphertext, and the decryption result is exactly the same as the given plaintext;

b) After the product uses the cryptographic algorithm to encrypt the given key and plaintext, it calls the cryptographic algorithm to perform a decryption operation, and the decryption result is exactly the same as the given plaintext.

For the signature/verification operation that support the SM2 algorithm:

a) After the product uses the given key to call the cryptographic algorithm to sign the message to be signed, the test platform verifies the signature result, and the verification passes;