GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

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

Issued on: November 20, 2022 **Implemented on: June 01, 2023**

Issued by: State Cryptography Administration

Table of Contents

Cryptography test specification for secure separation and information exchange product

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 Product management function test

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 Product status test

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 Product self-test test

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 Product configuration management test

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 Correctness and consistency of asymmetric cryptographic algorithms

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;

b) After the product uses the given key to call the cryptographic algorithm to sign the message to be signed, it calls the cryptographic algorithm to perform a verification operation, and the verification passes.

4.7.4 Correctness and consistency of hash cryptographic algorithm

4.7.4.1 Test requirements

If the product uses the hash cryptographic algorithm, it shall support the SM3 cryptographic algorithm, and its implementation shall comply with GB/T 32905.

4.7.4.2 Test method

The product calls the hash algorithm to calculate the hash value for a given message, and the result is exactly the same as the given hash value.

4.8 Product random number quality test

4.8.1 Test requirements

The random numbers generated and used by the product shall be provided by the cryptographic module, and the cryptographic module shall be certified by national commercial cryptography certification authority.

4.8.2 Test method

Call the product random number generation interface, and collect 1000 128 KB random number files; test the collected random number files, and the test results shall meet the requirements of GB/T 32915.

4.9 Product role identification test

4.9.1 Basic level requirements

4.9.1.1 Test requirements

Products with basic security level shall have roles and corresponding identification mechanisms, and different access or operations shall have different permissions. The product shall reject any access or operation that does not have the corresponding permissions to prevent unauthorized malicious personnel from logging in and undermining the security of the product.

4.9.1.2 Test method

The test method is as follows:

a) Enter the wrong username and random login password through the product management interface, and the login fails;

b) Enter the correct username and random login password through the product management interface, and the login fails;

c) Enter the correct username and correct login password through the product management interface, and the login is successful.

4.9.2 Enhanced level requirements

4.9.2.1 Test requirements

Products with enhanced security level shall use hardware devices such as smart password keys certified by national commercial cryptography certification authority to represent identity, and combine login passwords to implement a multi-factor authentication mechanism, where the password length shall be greater than 6 digits, and the password shall contain at least numbers, uppercase and lowercase letters, and may also contain special characters. The product shall implement an approved authentication mechanism specified in GB/T 15843.

4.9.2.2 Test method

f) Key recovery: use the product key management tool to perform the key recovery operation, and successfully restore it to the cryptographic module.

g) Key destruction: use the product key management tool to perform the key destruction operation, and successfully destroy the specified key.

4.11 Product log audit test

4.11.1 Test requirements

The product shall provide log recording, viewing and export functions, and shall be able to ensure that the log has not been illegally tampered with.

4.11.2 Test method

View the log content through the product management interface, which shall include:

a) Administrator operation behavior, including operations such as login authentication, configuration management;

b) Abnormal events, including records of abnormal events such as self-test failure and authentication failure.

The log content should include:

a) All attempts to modify security attributes, including the security attribute values before and after the modification;

b) The result data of the cryptographic algorithm correctness test, random number quality test, identification data, and key integrity self-test, including self-test items and test results.

4.12 Product function test

4.12.1 General requirements

The product shall realize secure data exchange between two security domains, and ensure that the two processing systems inside and outside the secure separation and information exchange product are not connected at the same time.

4.12.2 Basic level requirements

4.12.2.1 Test requirements

Products with basic security level shall comply with the provisions of 5.2.2.1.1.1 and 5.2.2.1.1.2 of GB/T 20279-2015.

4.12.2.2 Test method

The test method is as follows:

a) Simulate the information flow supported by the device, and all information flows between the sender and the receiver of the product shall implement the control strategy specified in 5.2.2.1.1.1 of GB/T 20279-2015;

b) Obtain the receiver's information flow data and verify that the product implements the control functions specified in 5.2.2.1.1.2 of GB/T 20279-2015.

4.12.3 Enhanced level requirements

4.12.3.1 Test requirements

Products with enhanced security level shall comply with the provisions of 5.2.2.2.1.1 and 5.2.2.2.1.2 of GB/T 20279-2015.

4.12.3.2 Test method

The test method is as follows:

a) Simulate the information flow supported by the device, and all information flows between the sender and the receiver of the product shall implement the control strategy specified in 5.2.2.2.1.1 of GB/T 20279-2015;

b) Obtain the receiver's information flow data and verify that the product implements the control function specified in 5.2.2.2.1.2 of GB/T 20279-2015.

4.13 Product performance test

The exchange rate and hardware switching time of the product shall comply with the provisions of 5.5 of GB/T 20279-2015.

5 Documentation requirements

5.1 System framework

Developers shall describe the system framework of the product in the form of a structure diagram, including the composition of each subsystem of the secure separation and information exchange product, the functions of each subsystem and the implementation principle of each subsystem, and attach detailed text descriptions.

Describe in detail the security mechanism, cryptographic system and key management of secure separation and information exchange products.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------