

ICS 35.030
CCS L 80

GM

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

GM/T 0121-2022

Test specification for cryptographic board

密码卡检测规范

(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
Initialization testing	3
Cryptographic algorithm testing	4
Key structure	5
Key generation and storage	6
Key import and export	7
Key usage and update	8
Key backup and recovery	9
Testing for random number quality	10
Application interface testing	11
Physical interface testing	12
Permission management	13
Equipment management	14

1 Scope

This document specifies the testing content, testing methods, testing requirements and documentation requirements for cryptographic board cards.

This document is applicable to the testing of cryptographic board cards and the development of such cryptographic devices, and can also be used to guide the development of applications based on such cryptographic devices.

2 Normative references

The provisions of the following documents constitute the essential clauses of this document through normative references in this text. Among them, for referenced documents with dates, only the versions corresponding to the dates are applicable to this document; for referenced documents without dates, the latest versions (including all amendments) are applicable to this document.

GB/T 15852.2 Cybersecurity technology - Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function
 GB/T 17964 Information security technology - Modes of operation for a block cipher
 GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm
 GB/T 32907 Information security technology - SM4 block

cipher algorithm GB/T 32918(all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 33133(all parts) Information security technology - ZUC stream cipher algorithm GB/T 33560 Information security technology - Cryptographic application identifier criterion specification GB/T 35275 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification GB/T 35276 Information security technology - SM2 cryptographic algorithm usage

- a) Function testing: initialization testing, cryptographic algorithm testing, key management testing, random number quality testing, interface testing, and management security testing;
- b) Performance testing: It includes the testing of random number generation performance, symmetric key generation performance, asymmetric key pair generation performance, symmetric algorithm encryption and decryption performance, asymmetric algorithm encryption and decryption performance, asymmetric algorithm signature and verification performance, and hash algorithm operation performance;
- c) Safety testing;
- d) Virtualization testing.

6.2.1 Initialization testing

Testing requirements:

- a) It shall be able to be correctly installed in the test platform, and its device driver shall be able to be correctly installed and uninstalled in the specified operating system;
- b) After powering on, the card shall perform a self-test (including cryptographic algorithms, random numbers, static storage data, software firmware integrity and other functional components that require self-test) and output status indications; if the power-on-self-test fails, the card shall refuse all cryptographic function call services;
- c) It shall support at least two states: initial and ready. A cryptographic board card without a device key pair and protection key installed is in the initial state, and a cryptographic board card with a device key pair and protection key installed is in the ready state. In the initial state, only device information can be read, administrators and operators can be added (if operator roles are supported), and device key pairs and protection keys can be generated or restored. In the ready state, except that the generation or restoration of device key pairs and protection keys cannot be performed, related operations can be performed according to role permissions; when administrator permissions are met, key management and cryptographic operations can be provided; when operator permissions are met, cryptographic operations can be provided. In the ready state, the cryptographic board card can be put into the initial state by restoring factory settings or resetting to zero.
- d) The driver should support the basic requirements of simultaneous use and operation of

multiple cryptographic board card devices and should have a secure binding mechanism with the cryptographic board card.

Testing steps:

- a) Insert the cryptographic board card into the testing server, and the driver shall be successfully installed or uninstalled;
- b) The cryptographic board card shall correctly perform hardware power-on-self-test and output the self-test status result; if the self-test status result shows that the self-test fails, the cryptographic function call service is further performed and the operation shall fail;
- c) If the device key pair and protection key are not installed, the device information shall be read successfully, the device key pair and protection key shall be generated or restored successfully, and any other security service or key management operation shall fail;
- d) Administrator and operator permissions shall be added through the management tool, and the device key pair and protection key shall be successfully generated (or restored) to enter the ready state;
- e) In the ready state, if the administrator identity authentication is not passed, the key management operation, cryptographic operation and other security service operations shall fail; if the administrator authority authentication is passed, the key management operation, cryptographic operation and other security service operations shall succeed;
- f) When the operator role is supported, in the ready state, if the operator identity authentication is not passed, the security service operations such as key management and cryptographic operations shall fail; after the operator identity authentication is passed, the security services such as cryptographic operations shall be successfully executed, and the key management operations shall fail;
- g) In the ready state, if operations such as restoring factory settings or triggering the key destruction mechanism are performed, and all keys and sensitive information in the cryptographic board card are set, the cryptographic board card enters the initial state;
- h) Check the driver file and verify the binding relationship between the driver and the cryptographic board card by obtaining the unique identifier inside the cryptographic board card through the driver.

6.2.2 Cryptographic algorithm testing

- 2) The given key and ciphertext are decrypted using the specified algorithm and working mode, and the result is exactly the same as the given plaintext.
- b) The cryptographic board card shall perform a hash operation on the message to detect the correctness of the operation result. For a given message and parameter (or null), the hash algorithm is called to calculate the hash value, and the result is exactly the same as

the given hash value.

c) The cryptographic board card shall use asymmetric cryptographic algorithms to encrypt and decrypt data, sign/verify, perform key agreement operations, and detect the correctness of the operation results:

- 1) After encrypting with the given key and plaintext using the cryptographic algorithm, the cryptographic algorithm is called to perform decryption operations, and the decryption result is exactly the same as the given plaintext;
- 2) After encrypting with the given key and plaintext using the cryptographic algorithm, the testing platform performs a decryption operation on the ciphertext, and the decryption result is exactly the same as the given plaintext;
- 3) After using the given key to call the cryptographic algorithm to sign the message to be signed, call the cryptographic algorithm to verify the signature value, and the verification passes;
- 4) After using the given key to call the cryptographic algorithm to sign the message to be signed, the testing platform verifies the signature value and the verification passes;
- 5) Using the given key and key agreement parameters, call the key agreement algorithm to perform the key agreement with the testing platform, and the result is correct.

d) The cryptographic board card shall correctly perform the power-on/reset self-test and periodic self-test of the cryptographic algorithm, and verify the self-test status results or status indications. If the self-test fails, the operation of calling the cryptographic board card to perform the cryptographic operation shall fail.

6.2.3.1 Key structure

The cryptographic board card shall have a complete key management function and shall support at least three levels of key structure:

-- The first level is the protection key, which is used to protect the security of other keys and sensitive information in the cryptographic board card, including the management of other keys.

-- The second level is user key pairs, key encrypting keys, and device key pairs.

User key pairs include signature key pairs and encryption key pairs, which are used to implement functions such as user digital signatures, signature verification, and session key protection; key encrypting keys are symmetric keys that are replaced regularly and are used to protect session keys; device key pairs, as the identity keys of cryptographic board cards, include signature key pairs and encryption key pairs, which are used for device management and are not open to upper-level applications.

-- The third level is the session key, which is used for data encryption and decryption.