

ICS 35.030  
CCS L 80

**GM**

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

**GM/T 0122-2022**

---

**Cryptography test specification for blockchain**

区块链密码检测规范

**(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  |
| Hash cryptographic algorithm implementation correctness test .....       | 3  |
| Asymmetric cryptographic algorithm encryption and decryption .....       | 4  |
| Asymmetric cryptographic algorithm digital signature and signature ..... | 5  |
| Asymmetric key pair consistency test .....                               | 6  |
| Random number test .....                                                 | 7  |
| Cryptographic protocol .....                                             | 8  |
| Key management .....                                                     | 9  |
| Cryptography test requirements for blockchain .....                      | 10 |
| Account creation .....                                                   | 11 |
| Real-name authentication .....                                           | 12 |
| Authentication .....                                                     | 13 |
| Transaction creation .....                                               | 14 |
| Transaction verification .....                                           | 15 |
| Off-chain transaction .....                                              | 16 |
| Communication security .....                                             | 17 |
| Consensus mechanism .....                                                | 18 |
| Smart contracts .....                                                    | 19 |
| Test scenario .....                                                      | 20 |
| System performance .....                                                 | 21 |

### 1 Scope

This document specifies the test content, test methods and qualification criteria for relevant cryptographic technologies in blockchain cryptographic modules.

This document applies to the test of blockchain cryptographic modules and can be used to guide the design of blockchain cryptographic modules and the use of cryptographic technologies.

## 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 15843.2, Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms  
 GB/T 15843.3, Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques  
 GB/T 15843.4, Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function  
 GB/T 15843.5, Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero knowledge techniques  
 GB/T 15852.2, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function  
 GB/T 20518, Information security technology - Public key infrastructure - Digital certificate format  
 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

b) Perform decryption operation on the given key and ciphertext according to the specified operation mode, and the result shall be exactly the same as the given plaintext.

### 6.1.3 Hash cryptographic algorithm implementation correctness test

For given messages and parameters, call the hash algorithm, to test the correctness of its operation results, including:

- a) Call the hash algorithm operation interface for the given message to calculate the hash value, and the result shall be exactly the same as the given hash value;
- b) Call the hash algorithm operation interface for the given message and parameters to calculate the hash value, and the result shall be exactly the same as the given hash value.

### 6.1.4 Asymmetric cryptographic algorithm encryption and decryption

implementation correctness test for the given key and plaintext (ciphertext), call the asymmetric cryptographic algorithm, to test the correctness of its operation results, including:

- a) Call the asymmetric cryptographic algorithm encryption operation interface to perform encryption operation on the given plaintext and key, and test the tool's decryption operation on the ciphertext. The decryption result shall be exactly the same as the given plaintext;

b) Call the asymmetric cryptographic algorithm decryption operation interface to perform decryption operation on the given ciphertext and key, and the decryption result shall be exactly the same as the given plaintext.

#### **6.1.5 Asymmetric cryptographic algorithm digital signature and signature**

verification implementation correctness test Call the asymmetric cryptographic algorithm to perform signature/verification operation on the data, and test the correctness of the operation results, including:

- a) Call the asymmetric cryptographic algorithm signature operation interface to perform signature operation on the given message to be signed and the key, and test the tool's verification operation on the signature result, where it shall pass the signature verification;
- b) Call the asymmetric cryptographic algorithm signature verification operation interface to perform signature verification on the given signature result, the message to be signed, and the key, where it shall pass the signature verification.

#### **6.1.6 Asymmetric key pair consistency test**

For the generated public and private keys, call the asymmetric cryptographic algorithm to test the correctness of the operation results, including:

- a) Use the public key to encrypt the plaintext, and use the private key to decrypt the ciphertext. The decrypted result shall be the same as the original plaintext;
- b) Test the asymmetric key pair consistency by calculating and verifying a digital signature, where the digital signature shall be verified.

#### **6.2 Random number test**

Random numbers shall be generated using cryptographic components or modules that have passed cryptographic testing and certification, and the quality of random numbers shall comply with the requirements of GM/T 0005.

#### **6.3 Cryptographic protocol**

The cryptographic protocols used shall comply with the relevant cryptographic requirements of national standards and industry standards:

- a) When using the TLCP protocol, it shall comply with GB/T 38636;
- b) When using IPSec protocol, it shall comply with GM/T 0022;
- c) When using zero knowledge proof, ring signature, group signature, secure multi-party computing, etc. that have been reviewed and authenticated by the national cryptography authorities, protocol interaction data shall be collected to verify correctness and

consistency.

## 6.4 Key management

Key management security shall meet the following requirements:

- a) The key generation shall be done inside the cryptographic component or module that has passed the cryptographic testing and certification; the generation and negotiation of private keys and symmetric keys shall use random numbers that meet the requirements of GM/T 0005;
- b) Symmetric keys and private keys shall be stored in a secure form or in encrypted form;
- c) If the key distribution process is involved, security measures such as identity authentication shall be in place to ensure the authenticity of the key;

cryptographic technologies such as digital signature and HMAC shall be used to ensure the integrity of the distributed key, where HMAC shall comply with GB/T 15852.2; security measures shall be in place to ensure the confidentiality of the key;

cryptographic machine, VPN, cryptographic smart token, timestamp server, signature verification server, etc.

## 7 Cryptography test requirements for blockchain

cryptographic modules

### 7.1.1 Account creation

Test requirements:

During the account creation phase, a transaction address that can identify the user shall be generated, and a public-private key pair of the SM2 algorithm shall be generated using a cryptographic component or module that has passed the cryptographic testing and certification. The user's private key shall be securely generated and stored inside the cryptographic module, which shall meet the relevant requirements of GM/T 0028.

Test steps:

- a) Simulate account creation process;
- b) Verify the public-private key pair mechanism for generating the SM2 algorithm during account creation, and verify whether the cryptographic components or modules that have passed the cryptographic testing and certification are used for generation;
- c) Verify and analyze whether the user's private key is generated and stored in a cryptographic component or module that has passed cryptographic testing and certification.

Result judgment: