GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

File No.: 58551-2017

GM/T 0046-2016

Test specification for financial cryptographic server

金融数据密码机检测规范

Issued on: December 23, 2016 **Implemented on: December 23, 2016**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of Code Industry Standardization Technical Committee.

The drafting organizations of this Standard: Wuxi Jiangnan Information Security Engineering Technology Center, State Cryptography Administration Commercial Cryptography Detection Center, Westone Information Industry Company Limited, Xing Tang Communication Technology Co., Ltd., Shandong De'an Information Technology Co., Ltd.

Main drafters of this Standard: Zhang Suocheng, Qi Chuanbing, Li Dawei, Deng Kaiyong, Luo Peng, Li Guoyou, Liu Chang, Xiao Qiulin, Ding Yuquan, Liu Xianxaing, Li Yuanzheng, Wang Nina, Kong Fanyu.

Test specification for financial cryptographic server

1 Scope

This Standard specifies the test requirements and test methods for financial cryptographic server.

This Standard is applicable to the detection of financial cryptographic server as well as the development of this type of cryptographic device.

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 32915, *Information security technology - Binary sequence randomness detection method*

GM/T 0028, *Security Requirements for Cryptographic Modules*

GM/T 0039, *Security Test Requirements for Cryptographic Modules*

GM/T 0045-2016, *Specifications of financial cryptographic server*

GM/T 0050, *Code device management - Device management technical specification*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 financial cryptographic server

a cryptographic device that is used in finance field to protect financial data security, mainly for PIN encryption, PIN trans-encryption, MAC generation and check, data encryption and decryption, signature verification as well as key management and other cryptographic services

3.2 symmetric cryptographic algorithm

a cryptographic algorithm that encryption and decryption use same key a hash algorithm with its output of 256 bits

3.11 SM4 algorithm

a block cryptographic algorithm with group length of 128 bits, key length of 128 bits

3.12 physical secure environment; PSE

an environment with access control mechanisms or other security mechanisms; it is designed to prevent partial or total leakage of key, or leakage of other private data stored in the environment, such as any unauthorized access, for example, room or security entity with uninterrupted access control, physical security protection and monitoring

3.13 physical protection; PP

physically secure the hardware cryptographic device and its keys or sensitive information, for example, using prying resistance means to prevent the cryptographic server being unauthorized opened

3.14 master key; MK

in the hierarchy of the key encryption key and the transmission key, the highest-level key encryption key is called a master key, also known as master file key or local master key

3.15 key separation; KS

ensure that each cryptographic operation uses only the specified key type, for example, the MAC key can only be used to generate a message authentication code

3.16 data key; DK

a key that is to protect PIN and calculate MAC, including MAC key (MAK) and PIN key (PINK), also known as working key

3.17 check value; CV

through the result value calculated by irreversible algorithm, the check value usually transforms a random string of results under a key; in the case of an unknown key, it is not feasible to calculate the correct check value, and a key cannot be determined by the check value

3.18 personal identification number; PIN

in financial business, a digital ID that authorizes a cardholder in a request for authorization message; PIN only contains decimal number

b) with power indicator light;

c) with state indicator light;

d) with failure indicator light;

e) with at least one service port;

f) with at least one management port;

g) if the key storage uses micro-protection memory, it shall have a key self-destruction mechanism.

The financial cryptographic server shall have the following components or ports:

a) one printing port is preferred;

b) if the key is used in plaintext in the financial cryptographic server memory, it shall have a memory cleaning mechanism;

c) a chassis shell grounding device is preferred;

d) redundant power supply is preferred;

e) IC card socket is preferred;

f) USB port is preferred;

g) human-computer interaction component is preferred.

6.3 Function test

6.3.1 Initialization test

The financial cryptographic server shall have initialization function to realize the switching between initial state to working state of the device.

The initial operation of the financial cryptographic server mainly includes initial system configuration, initializing the administrator or operator, initial key generation (or recovery) and installation. The financial cryptographic server provides cryptographic services only after the initialization operation is completed. After initial configuration of the financial cryptographic server, it can automatically enter the working state to provide cryptography service.

If the initial configuration is not performed, when the financial cryptographic server starts up, it shall alarm via indicator light and sound to prompt user to initialize. At this moment, the financial cryptographic server cannot provide cryptography service.

k) SM2 key agreement.

The test methods for cryptographic operation of financial cryptographic server:

a) SM4 ECB encryption: encrypt the given key and plaintext through ECB mode, the result shall be exactly same with the given ciphertext;

b) SM4 ECB decryption: decrypt the given key and ciphertext through ECB mode, the result shall be exactly same with the given plaintext;

c) SM4 CBC encryption: encrypt the given IV, key and plaintext through CBC mode, the result shall be exactly same with the given ciphertext;

d) SM4 CBC decryption: decrypt the given IV, key and plaintext through CBC mode, the result shall be exactly same with the given plaintext;

e) SM3 hash: call SM3 algorithm for given information to calculate the hash value, the result shall be exactly same with the given hash value;

f) SM2 key generation: call financial cryptographic server to generate a SM1 key pair, then use its private key pair to sign the designated data; then the test platform shall use its public key to verify whether the signature result is correct;

g) SM2 signature: call SM2 signature function of financial cryptographic server to sign the designated data for several times; the test platform shall inspect:

1) whether the signature result is correct;

2) the signature result shall be different each time;

h) SM2 signature verification: the test platform performs SM2 signature, calls SM2 signature verification function of financial cryptographic server to inspect:

1) the correct signature shall be verified as passed;

2) the wrong signature shall be verified as failed;

i) SM2 encryption: call SM2 encryption function of financial cryptographic server to encrypt the designated data for several times; the test platform shall inspect:

1) whether the encryption result is correct;

2) the encryption shall be different each time;

j) SM2 decryption: the test platform performs SM2 encryption, calls SM2

b) cryptographic service program reboots the record, records the event of cryptographic service program reboot due to program BUG or memory overflow and other reasons, including the reboot time, the system state;

c) other abnormal events, such as abnormal port connection, insufficient system resources.

6.3.8 Device self-test

The device self-test function of financial cryptographic server shall mainly include cryptographic algorithm correctness test, random number quality test generated by random number generator, integrity test of stored key and data as well as correctness test of key components.

The financial cryptographic server shall support power-on / reset self-test, manual self-test and periodic self-test functions.

The power-on / reset self-test shall be automatically performed after each power-on / reset starts. If the self-test is successful, the financial cryptographic server shall automatically enter management state or operation state. If the self-test fails, the financial cryptographic server shall report the test results and stop providing cryptographic service externally.

The manual self-test shall be performed through management interface after the financial cryptographic server starts up. The test results shall be reported after self-test ends.

The periodic self-test shall be automatically performed according to the set period during the operation process of financial cryptographic server. If the self-test fails, the financial cryptographic server shall report the test results and stop providing cryptographic service externally.

6.3.9 Data message interface detection

The test platform shall test the application program interfaces specified by GM/T 0045-2016 one by one. Only when the tests of all interfaces are correct, it shall pass the test.

a) With correct calling environment and calling process, API function shall return correct result and complete corresponding functions;

b) With wrong calling environment and calling process, API function shall return corresponding error codes.

item. The test number N is required not too small so as to ensure the precision of test result. Meanwhile, N cannot be too large so as to avoid test time too long.

6.4.2 PIN encryption performance test

Perform encryption operation for a PIN. Repeat N times. Measure the completion time T. The data used for test shall be selected by the testing organization. The test shall be carried out for several times. Take mean value as result. The unit for PIN encryption performance shall be tps (time per second).

The financial cryptographic server shall support SM4 PIN encryption.

6.4.3 PIN trans-encryption performance test

Trans-encrypt a PIN block that is protected by LMK to a PIN block protected by ZPK. Repeat N times. Measure the completion time T. The data used for test shall be selected by the testing organization. The test shall be carried out for several times. Take mean value as result. The unit for PIN trans-encryption performance shall be tps (time per second).

The financial cryptographic server shall support SM4 PIN trans-encryption.

6.4.4 MAC calculation performance test

Calculate a random MAC value of 256 bytes data. Repeat N times. Measure the completion time T. The data used for test shall be selected by the testing organization. The test shall be carried out for several times. Take mean value as result. The unit for MAC calculation performance shall be tps (time per second).

The financial cryptographic server shall support SM4 MAC calculation.

6.4.5 ARQC verification performance test

Verify a ARQC value. Repeat N times. Measure the completion time T. The data used for test shall be selected by the testing organization. The test shall be carried out for several times. Take mean value as result. The unit for ARQC verification performance shall be tps (time per second).

The financial cryptographic server shall support SM4 ARQC verification.

6.4.6 Encryption and decryption performance test of symmetric cryptographic algorithm

Encrypt / decrypt a fixed-length data message. Repeat N times. Measure the completion time T. The data used for test shall be selected by the testing organization. The test shall be carried out for several times. Take mean value as result. The unit for encryption and decryption performance of symmetric

Annex A

(normative)

Test item list

Table A.1 -- Appearance and structure test items

Test item	Test content	Remark
Appearance and structure inspection	The panel printing is required clear, signs pasted firm, no obvious scratch on whole casing, with complete accessories.	
	The financial cryptographic server shall have the following main components or ports: a) with power indicator light; b) with state indicator light; c) with failure indicator light; d) with at least one service port; e) with at least one management port; f) if the key storage uses micro-protection memory, it shall have a key self-destruction mechanism.	
	The financial cryptographic server shall have the following main components or ports: a) one printing port is preferred; b) if the key is used in plaintext in the financial cryptographic server memory, it shall have a memory cleaning mechanism; c) a chassis shell grounding device is preferred; d) redundant power supply is preferred; e) IC card socket is preferred; f) USB port is preferred; g) human-computer interaction component is preferred.	

Table A.2 -- Initialization test items

Test item	Test content	Remark
Initialization test	If no initialization, whether it prompts to alarm.	
	After the initialization is executed, whether it can enter working state.	
	Generation of administrator	
	Configuration of service port	
	Configuration of management port	

Bibliography

[1] GB/T 4943-1995, *Safety of information technology equipment including electrical business equipment*

[2] GB/T 9813-2000, *Specification for microcomputer*

[3] GB/T 17903.1-1999, *Information technology - Security techniques - Non-repudiation - Part 1: General*

[4] GB/T 17903.2-1999, *Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*

[5] GB/T 17903.3-1999, *Information technology- - Security techniques - Non-repudiation - Part 3：Mechanisms using asymmetric techniques*

[6] GB/T 17964-2000, *Information technology - Security techniques - Encryption algorithm - Part 1: General*

[7] GB/T 17964-2000, *Information technology - Security techniques - Encryption algorithm - Part 2: Asymmetric encryption*

[8] GB/T 17964-2000, *Information technology - Security techniques - Encryption algorithm - Part 3: Symmetric encryption*

[9] GB/T 17964-2008, *Information technology - Security techniques - Modes of operation for an n-bit block cipher*

[10] GB/T 18336-2001, *Information technology - Security techniques - Evaluation criteria for IT security*

[11] GB/T 18238.1-2000, *Information technology - Security techniques-Hash-function - Part 1: General*

[12] GB/T 18238.2-2002, *Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher*

[13] GB/T 18238.3-2002, *Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions*

[14] GB/T 32905-2016, *Information security technology SM3 cryptographic hash algorithm*

[15] GB/T 32907-2016, *Information security techno1ogy - SM4 b1ock cipher algorithm*

[16] GB/T 32918.1-2016, *Information security techniques - Elliptic Curve public - key cryptography - Part 1: General*

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

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