GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

File No.: 55613-2016

GM/T 0045-2016

Specifications of financial cryptographic server

金融数据密码机技术规范

Issued on: March 28, 2016 **Implemented on: March 28, 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.

Main drafting organizations of this Standard: Chengdu Westone Information Industry Joint Stock Company, Wuxi Jiangnan Institute of Computer Technology, Xing Tang Communication Technology Co., Ltd., Shandong De'an Information Technology Co., Ltd., Beijing Sansec Technology Development Company, Ltd., Beijing Jiangnan Tian-An Technology Co., Ltd.

Main drafters of this Standard: Li Yuanzheng, Zhang Shixiong, Huang Jin, Zhang Suocheng, Xu Mingyi, Wang Nina, Zheng Haisen, Gao Zhiquan, Li Guo, Ma Xiaoyan.

Specifications of financial cryptographic server

1 Scope

This Standard defines relevant terms of financial cryptographic server, specifies functional requirements, interface requirements, hardware requirements, business requirements, security requirements and test requirements for financial cryptographic server.

This Standard is applicable to the development, use of financial cryptographic server. It is also applicable to guide the test of financial cryptographic server.

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 4943, *Safety of information technology equipment*

GB/T 9813-2000, *Specification for microcomputer*

GB/T 17964, *Information technology - Security techniques - Modes of operation for a block cipher*

GM/T 0002, *SM4 Block Cipher Algorithm*

GM/T 0003, *Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves*

GM/T 0004, *SM3 Password Hashing Algorithm*

GM/T 0005, *Randomness Test Specification*

GM/T 0006, *Cryptographic application identifier criterion specification*

GM/T 0009, *SM2 Cryptography Algorithm Application Specification*

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

JR/T 0025, *China Financial Integrated Circuit Card Specifications*

use physical means to protect hardware cryptographic device and its keys or sensitive information

3.9 master key; MK

it is at the highest layer in hierarchical key structure, used to protect its lower keys

3.10 secondary master key; SMK

it is at the second layer in hierarchical key structure, used to generate or protect its lower keys

3.11 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

3.12 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

3.13 key check value; KCV

through the result value calculated by irreversible algorithm, it is used to for integrity inspection; the check value usually uses irreversible algorithm to calculate the result of any string under the key

3.14 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; when logging in, it can support numbers, uppercase and lowercase letters, punctuation

3.15 key loading; KL

a process of transferring keys to cryptographic server manually or electronically

3.16 manual key distribution; MKD

a method of using non-electronic means such as cryptography envelope for key distribution

3.17 manual key entry; MKE

inject keys with keyboard into financial cryptographic server

5 Functional requirements

5.1 Cryptographic algorithm

5.1.1 Symmetric cryptographic algorithm

The financial cryptographic server shall be equipped with SM4 symmetric cryptographic algorithm. The realization of SM4 cryptographic algorithm shall follow GM/T 0002.

In order to meet the requirement of compatibility with the original system or the interconnection with other systems (for example, the external card system), the international standard DES/3DES/AES cryptographic algorithm and other algorithms approved by the national cryptography management department may also be supported.

The operation mode of symmetric cryptographic algorithm shall follow GB/T 17694, at least containing ECB and CBC modes.

The symmetric cryptographic algorithm is mainly used for PIN encryption, PIN trans-encryption, MAC calculation, data encryption and decryption, key protection.

5.1.2 Public key algorithm

The financial cryptographic server shall be equipped with SM2 asymmetric cryptographic algorithm. The realization of SM2 cryptographic algorithm shall follow GM/T 0003. The use of algorithm shall follow GM/T 0009.

In order to meet the requirement of compatibility with the original system or the interconnection with other systems (for example, the external card system), the international standard RSA cryptographic algorithm and other algorithms approved by the national cryptography management department may also be supported. RSA cryptographic algorithm module length shall meet the length that is proposed and recommended by the international bank card organization. And it can be extended.

The asymmetric cryptographic algorithm is mainly sued for digital signature and signature verification, cryptography envelope, key distribution.

5.1.3 Hash algorithm

The financial cryptographic server shall be equipped with SM3 hash algorithm. The realization of SM3 hash algorithm shall follow GM/T 0004. In addition, when SM2 cryptographic algorithm is used for digital signature verification and calculation of message authentication code, the algorithm is required to equip with SM3 hash algorithm. The realization of SM3 hash algorithm used in SM2

information is not leaked.

The key in plaintext form that requires manual entry shall use segment transmission, storage and entry. Different key components shall be saved separately by different authorized administrators. During key entry, it shall be completed together by at least more than 2 authorized administrators on the entry site.

5.2.5 Key backup / restore

The financial cryptographic server shall have backup / restore function for master key, secondary master key. The backup data generated by the backup operation shall be stored in ciphertext on the storage medium. The key to encrypt the backup data shall have a security mechanism to ensure its security.

The backup key can be restored to the financial cryptographic server. Different models of financial cryptographic server of same manufacturer shall be able to backup and restore each other. The key restore can be only performed in the financial cryptographic server.

5.3 Random number

The financial cryptographic server shall use random numbers generated by no less than two hardware physical noise sources. The generated random numbers shall meet the requirements of GM/T 0005.

The random number generator equipped for financial cryptographic server shall pass four phrases of random number tests: sample sending test, exit-factory test, power-on test and use test.

a) Sample sending test

Carry out sample sending test of random number according to GM/T 0005 requirements.

b) Exit-factory test

- test quantity: collect 50×10^6 bit random numbers, divided into 50 groups, 106 bits for each group;
- test item: in accordance with GM/T 0005 requirements;
- test passing criteria: should any item of the test fail to pass the test criteria, it shall alarm that the test is failed; it allows to repeat one random number collection and test; if the repeated test still fails, the product's random number generator shall be determined as failed.

c) Power-on test

be completed by authorized administrator. The financial cryptographic server shall provide an administrator authentication mechanism.

The financial cryptographic server shall provide the network access control mechanism. The security officer shall configure the security policy that allows access to the cryptographic server. At least, it shall have the function of verifying the legal host's bile address.

5.5 Device management

5.5.1 Device self-test

The financial cryptographic server shall provide device self-test function. The self-test includes cryptographic algorithm correctness check, random number generator check, storage key and data integrity check.

5.5.2 Log audit

The financial cryptographic server shall provide logging capabilities while providing log viewing and log exporting capabilities. A log shall contain the main body of the log, log generation time. The log is divided into the following three categories of management:

a) log operation: record the operation of the administrator, including changes to the system configuration parameters;

b) log management: record the security events to be audited, including administrator login, key injection, key generation, key update, key destruction, authorization status switch;

c) log running: record the operating status of the device, including the device anomaly, rejection, alarm.

5.5.3 Remote management

When there is a need for remote centralized management, the financial cryptographic server shall have remote centralized management of the device. The realization of device management functions shall meet the requirements of relevant cryptographic device management practices.

5.6 Device initialization

The initialization of financial cryptographic server shall include administrator generation and authorization, system configuration by administrator according to authorization, key generation and installation, key backup.

The device initialization cannot be performed by manufacturer.

of the cryptographic operation of the financial cryptographic server with the known correct result. If the calculated result is the same as the correct result, the test passes; otherwise, the test fails.

The range of cryptographic operation test shall include each function provided by each symmetric cryptographic algorithm, asymmetric cryptographic algorithm and hash algorithm provided by the financial cryptographic server, such as encryption, decryption, hash, digital signature, signature verification, of which symmetric cryptographic algorithm test shall test the supported cryptographic algorithm operation patterns such as ECB, CBC, etc. The test results of cryptographic operation test shall meet 5.1 requirements.

9.1.3 Key management test

The key management test range includes key generation, key injection, key import / export, key backup / recovery / archive operation, testing with the management tools provided. The results of key management test shall meet 5.2 requirements.

9.1.4 Random number test

The random number test program shall be designed and provided by the testing organization approved by national cryptography management authority. The random number bit stream generated by financial cryptographic server is used as test sample and input into the random number test procedures to test the mass of random number. The random number test results shall meet 5.3 and 6.3 requirements.

9.1.5 Access control test

Use equipped management tools or manage interface of financial cryptographic server for the access control test. Different management operations shall be set to different operation permission. The management tool that logs in the financial cryptographic server shall have a sound identity authentication mechanism. The financial cryptographic server shall reject any unauthorized access or operation. The access control test results of financial cryptographic server shall meet 5.4 requirements.

9.1.6 Device management test

Use equipped management tools or manage interface of financial cryptographic server for the device management test, including system configuration, generation of administrator or operator, key management. The realization of device management function shall comply with relevant management regulation of cryptographic device. The device management test results shall meet 5.5 requirements.

$$S = N / T$$

where, S is speed, in times per second (tps); N is test times; T is measurement consumed time, in seconds (s).

9.2.2 PIN encryption performance test

Encrypt one PIN. Repeat N times. Measure its completion time T. The data used for test is set by testing organization. The test shall be performed several times. Take mean value as result.

The unit for PIN encryption performance shall be times per second (tps) in uniform.

9.2.3 Trans-encryption performance test

Trans-encrypt one PIN block protected by LMK to PIN block protected by ZPK. Repeat N times. Measure its completion time T. The data used for test is set by testing organization. The test shall be performed several times. Take mean value as result.

The unit for PIN trans-encryption performance shall be times per second (tps) in uniform.

9.2.4 MAC calculation performance test

Calculate the MAC value of a random 256-byte data. Repeat N times. Measure its completion time T. The data used for test is set by testing organization. The test shall be performed several times. Take mean value as result.

The unit for MAC calculation performance shall be times per second (tps) in uniform.

9.2.5 ARQC authentication performance test

Verify an ARQC value. Repeat N times. Measure its completion time T. The data used for test is set by testing organization. The test shall be performed several times. Take mean value as result.

The unit for ARQC authentication performance shall be times per second (tps) in uniform.

9.2.6 Encryption and decryption performance tests of symmetric cryptographic algorithm

Encrypt / decrypt a fixed-length data message. Repeat N times. Measure its completion time T. The data used for test is set by testing organization. The test shall be performed several times. Take mean value as result.

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

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