GM

CRYPTOGRAPHY INDUSTRYSTANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L80
File No.: 44631-2014

GM/T 0030-2014

Cryptographic server technical specification

服务器密码机技术规范

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Cryptographic server technical specification

1 Scope

This standard defines the relevant terms of cryptographic server, and specifies other related content of cryptographic server, such as functional requirements, hardware requirements, software requirements, security requirements and test requirements.

This standard applies to the development and usage of cryptographic server, and it can also be used to guide the test of cryptographic server.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 9813 Generic specification for microcomputers

GM/T 0005 Randomness test specification

GM/T 0018 Cryptographic equipment application interface specification

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

Cryptographic server

It is also known as host encryption server; it is the equipment which can provide independently or in parallel multiple application entities with cryptographic service and key management.

3.2

Symmetric cryptographic algorithm

It is a cryptographic algorithm which uses the same key to encrypt and decrypt.

key-pair and encryption key-pair. It is used for device management to represent the identity of cryptographic server.

Key encryption key: It is symmetric key that is periodically replaced to protect session key in the case of a pre-assigned key. Cryptographic server may choose to support key encryption key.

Session key: It is used for data encryption-decryption.

5.3.3 Key generation and installation

Manager key: It is generated or installed by the management tool which is used in device initialization; it is stored in a secure storage area inside cryptographic server.

User key: User key consists of signature key and encryption key. Signature key is generated or installed by cryptographic server; it must support the use of physical noise source chip to generate, and it must support the use of strong prime numbers. Encryption key is issued by key management system to the device; the format for issuing the encryption key follows the rules for the protection format of the encryption key given in GM/T 0018; and the storage area for a certain number of user key-pairs must be supported according to the system requirements. The private key of user key-pairs must support hardware internal secure storage; it is appropriate to support the security access control of private key access password.

Device key: Device key consists of signature key and encryption key. Signature key is generated or installed by using management tool when the device is initialized; encryption key is issued by key management system to the device. Device key stores the security storage area inside cryptographic server.

Key encryption key: It is generated or installed by cryptographic equipment management tool, which must support the generation of physical noise source chips; the storage area for a certain number of key encryption key must be supported according to the system requirements; this key must support the secure storage inside cryptographic server.

Session key: It must support to use the generation of physical noise source chips to ensure the quality of session key; it must support that one session replaces one session key. Cryptographic server must not be exported in plaintext. When session key is stored for a long time, it must support the security protective measures of user key-pair or key encryption key for encrypted storage.

5.3.4 Key usage

Symmetric key: According to symmetric key index-number or other key unique

interface, management operations can be carried out, such as key generation, installation, backup, recovery, and log query.

Management personnel shall be identified into the management interface.

Different management operations shall have different operating authorization.

5.6 Device management

It is appropriate for cryptographic server to have the management function of accepting management center; the implementation of device management function shall be carried out according to the requirements of state cryptography administration competent department.

5.7 Log audit

Cryptographic server shall provide the function of log recording, log viewing and log exporting.

Log content includes:

a) Administrator operation behavior, including login authentication, system configuration and key management;

b) Abnormal events, including records of abnormal events, such as authentication failure and unauthorized access;

c) If it is connected to equipment management center, record the corresponding operation.

5.8 Equipment self-test

Cryptographic server shall have the function of self-test at power-on and when receiving self-test command.

Self-test function of equipment shall include the correctness checking of cryptography algorithm, the test of random-number generator and the test of storage key and data integrity.

6 Hardware requirements of cryptographic server

6.1 External interface

Cryptographic server shall provide service interface and management interface respectively.

It supports external RJ-45 Ethernet interface, serial interface, fiber channel, USB and other hardware interface protocols of current mainstream servers. It

- Test items: Test the collected random-numbers according to the 12 item-tests of GM/T 0005, except for discrete Fourier test, linear complexity test, universal statistical test.

- Test-pass standard: If one item fails to pass the standard during the test, warn that the test is not qualified.

  The repetition of random-number collection and test is allowed for only once; if it is still not qualified through repeated test, determine random-number generator of products to lose efficacy.

- Test cycle: It is configurable; test interval is at most 12 h.

2) One-time test

- Test quantity: It is determined according to the size of random-number which is collected in practical application each time, but the length shall not be less than 128 bits; moreover, the unused sequence that has passed the test may continue to be used.

- Test items: Poker test. When the sample length is less than 320 bits, the parameter m = 2.

- Test-pass standard: If one item fails to pass the standard during the test, warn that the test is not qualified.

  The repetition of random-number collection and test is allowed for only once; if it is still not qualified through repeated test, determine random-number generator of products to lose efficacy.

6.3 Environmental adaptability

The working environment of cryptographic server shall follow the requirements about “Climate and Environment Adaptability” in GB/T 9813 according to actual demand.

6.4 Reliability

The mean time between failures of cryptographic server shall not be less than 10000 h.

7 Software requirements of cryptographic server

7.1 Basic requirements

The underlying software of cryptographic server shall adopt modular design, prevent user's illegal calls through technical measures.

8.3 System requirements

The operating system which is used by cryptographic server shall be securely reinforced; cut down all unneeded modules and shut down all unneeded ports and services.

8.4 Use requirements

cryptographic server only accepts valid operating instructions.

8.5 Management requirements

8.5.1 Remote management

The remote management function of cryptographic server can only be used for remote monitoring, including queries of parameters and status. Other management functions do not allow remote management. Remote management shall be carried out in accordance with the requirements of state cryptography administration competent department.

8.5.2 Administrator security management

cryptographic server shall set administrators who can conduct management operations if they meet the corresponding administration authority.

Administrators shall have the hardware devices of identity information and pass identity authentication before conduct management operations.

Have the log audit function on management operations.

8.5.3 Device security management

8.5.3.1 Device initialization

The initialization of cryptographic server, in addition to the necessary operation of manufacturer, the system configuration, the key generation and management, the generation of administrators shall be completed by device administrative staff of user side.

8.5.3.2 Device test

Test the correctness of key components such as crypto-operation components.

Test the integrity of sensitive information such as stored keys.

When the test fails, give an alarm and stop working.

9.3.6.2 Local management test

Local management test of cryptographic server is performed by using management interface of cryptographic server, including system configuration, administrator generation, key generation and management of cryptographic server. The implementation of the local management function of cryptographic server shall comply with the requirements of state cryptography administration competent department. The test results of the local management test of cryptographic server shall meet the requirements of 5.6, 8.5.2 and 8.5.3.

9.3.7 Log audit test

Log audit test of cryptographic server is performed by using log management tool or interface of cryptographic server. Cryptographic server shall provide the functions of log recording, log viewing and log exporting. The log content of cryptographic server includes: operation behaviors of administrator, including the following operations, such as login authentication, system configuration, and key management; and abnormal events, including records of abnormal events, such as authentication failure and unauthorized access. The test results of log audit test on cryptographic server shall meet the requirements of 5.7.

9.3.8 Test of equipment self-test

The equipment self-test function of cryptographic server mainly includes the correctness checking of cryptographic algorithm, the test of random-number generator, the integrity test of storage key and data, and the correctness checking of key components. The test results of the equipment self-test on cryptographic server shall meet the requirements of 5.8 and 8.5.3.2.

9.3.9 Application Program Interface (API) Test

Application program interface of cryptographic server must follow GM/T 0018. Perform the test of application program interface on cryptographic server: for the correct calling environment and calling process, the API function shall return the correct result and perform the corresponding function; for the set incorrect calling environment and calling process, the API function shall return the corresponding wrong code.

9.3.10 Management tool test

The management tool test of cryptographic server is performed by using management tool or management interface of cryptographic server. Perform the management tool test on cryptographic server. The test results shall be consistent with the requirements of 7.3.

Encryption-decryption performance unit of symmetric cryptographic algorithm is unified as Mbit/s (megabits per second).

9.4.2 Encryption-decryption performance test of asymmetric cryptographic algorithm

Send a fixed-length data message to cryptographic server for encryption-decryption operation, and repeat the operation for N times to measure the completion time T. The data used for testing is selected by testing organization; the test shall be repeated for several times and average the result.

If cryptographic server supports a variety of asymmetric algorithms, test all the supported asymmetric cryptographic algorithm and its various application modes.

Encryption-decryption performance unit of asymmetric cryptographic algorithm is unified as tps (times/second).

9.4.3 Performance test of data hash algorithm

Send a fixed-length data message to cryptographic server for digest operation, and repeat the operation for N times to measure the completion time T. The data used for testing is selected by testing organization; the test shall be repeated for several times and average the result.

Performance unit of data hash algorithm is unified as Mbit/s (megabits per second).

9.4.4 Performance test of random-number generator

Let cryptographic server generate and output N group of random sequences which accord with random characteristics with a length of L; measure its completion time T. The test shall be repeated for several times and average the result.

Performance unit of random-number generator is unified as Mbit/s (megabits per second).

9.4.5 Performance test of asymmetric key generation

Let cryptographic server generate and output a specified number of key-pairs; measure its completion time T. The test shall be repeated for several times and average the result.

Performance unit of asymmetric key generation is unified as tps (times/second).

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

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